SIEMENS

SIMATIC NET

SCALANCE S y SOFTNET Security Client

Instrucciones de servicio

Prólogo

Introducción y fundamentos 1

Propiedades del producto y puesta en servicio 2

GETTING STARTED 3

Configuración con Security Configuration Tool 4

Firewall, Router y otras propiedades del módulo 5

Comunicación segura en la VPN a través de túnel IPsec (S612/S613) 6

SOFTNET Security Client (S612/S613) 7

Funciones online - Test, Diagnóstico y Logging 8

Consejos y ayuda A

Informaciones sobre la identificación CE B

Bibliografía C

Esquema acotado D

Historia del documento E

02/2011

C79000-G8978-C196-07

Notas jurídicas

Filosofía en la señalización de advertencias y peligros

Este manual contiene las informaciones necesarias para la seguridad personal así como para la prevención de daños materiales. Las informaciones para su seguridad personal están resaltadas con un triángulo de advertencia; las informaciones para evitar únicamente daños materiales no llevan dicho triángulo. De acuerdo al grado de peligro las consignas se representan, de mayor a menor peligro, como sigue.

⚠PELIGRO

Significa que, si no se adoptan las medidas preventivas adecuadas **se producirá** la muerte, o bien lesiones corporales graves.

⚠ADVERTENCIA

Significa que, si no se adoptan las medidas preventivas adecuadas **puede producirse** la muerte o bien lesiones corporales graves.

⚠PRECAUCIÓN

con triángulo de advertencia significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse lesiones corporales.

PRECAUCIÓN

sin triángulo de advertencia significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse daños materiales.

ATENCIÓN

significa que puede producirse un resultado o estado no deseado si no se respeta la consigna de seguridad correspondiente.

Si se dan varios niveles de peligro se usa siempre la consigna de seguridad más estricta en cada caso. Si en una consigna de seguridad con triángulo de advertencia se alarma de posibles daños personales, la misma consigna puede contener también una advertencia sobre posibles daños materiales.

Personal cualificado

El producto/sistema tratado en esta documentación sólo deberá ser manejado o manipulado por **personal cualificado** para la tarea encomendada y observando lo indicado en la documentación correspondiente a la misma, particularmente las consignas de seguridad y advertencias en ella incluidas. Debido a su formación y experiencia, el personal cualificado está en condiciones de reconocer riesgos resultantes del manejo o manipulación de dichos productos/sistemas y de evitar posibles peligros.

Uso previsto o de los productos de Siemens

Considere lo siguiente:

⚠ADVERTENCIA

Los productos de Siemens sólo deberán usarse para los casos de aplicación previstos en el catálogo y la documentación técnica asociada. De usarse productos y componentes de terceros, éstos deberán haber sido recomendados u homologados por Siemens. El funcionamiento correcto y seguro de los productos exige que su transporte, almacenamiento, instalación, montaje, manejo y mantenimiento hayan sido realizados de forma correcta. Es preciso respetar las condiciones ambientales permitidas. También deberán seguirse las indicaciones y advertencias que figuran en la documentación asociada.

Marcas registradas

Todos los nombres marcados con ® son marcas registradas de Siemens AG. Los restantes nombres y designaciones contenidos en el presente documento pueden ser marcas registradas cuya utilización por terceros para sus propios fines puede violar los derechos de sus titulares.

Exención de responsabilidad

Hemos comprobado la concordancia del contenido de esta publicación con el hardware y el software descritos. Sin embargo, como es imposible excluir desviaciones, no podemos hacernos responsable de la plena concordancia. El contenido de esta publicación se revisa periódicamente; si es necesario, las posibles las correcciones se incluyen en la siguiente edición.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
ALEMANIA

Referencia del documento: C79000-G8978-C196-07
℗ 02/2011

Copyright © Siemens AG 2006, 2007, 2008, 2010, 2011.
Sujeto a cambios sin previo aviso

Prólogo

Este manual...

...le ayuda a poner en servicio el Security Module SCALANCE S602 / S612 / S613 así como el SOFTNET Security Client. Las variantes SCALANCE S602 / S612 / S613 reciben a partir de ahora la denominación SCALANCE S.

Nuevo en esta edición

En esta edición se consideran, entre otras cosas, las siguientes nuevas funciones:

- **Security Configuration Tool V2.3**

  Para conseguir un fácil acceso y una mejor visión de conjunto de los diferentes tipos de módulos, se ha cambiado el concepto de gestión de la integración y el intercambio de módulos.

  Se puede configurar un SOFTNET Security Client V3.0 junto con un MD741-1 y generar los correspondientes archivos de configuración (véase GETTING STARTED Ejemplo 5: Acceso remoto - ejemplo de túnel VPN con MD741-1 y SOFTNET Security Client (Página 87)).

  En el modo IKE (fase 1) se pueden parametrizar los algoritmos de encriptación AES-128, AES-192 y AES-256.

  Además de los sistemas operativos Windows XP SP2 y Windows XP SP3, es también compatible el sistema operativo Windows 7 (no la versión Home).

- **SOFTNET Security Client V3.0**

  Para una mejor visualización y diagnóstico de los estados de las conexiones, se han implementado nuevos iconos y se ha agregado una vista adicional de diagnóstico ("Diagnóstico ampliado").

  Para la consola de log de la vista de túnel se pueden realizar ajustes teniendo en cuenta los mensajes que se van a mostrar y el tamaño de los archivos de log.

  Para ahorrar costes en las conexiones orientadas al volumen, cabe la posibilidad de desactivar el test de accesibilidad reduciendo la capacidad diagnóstica del SOFTNET Security Client V3.0.

  En el diagnóstico de la accesibilidad de los partner de tunneling, en el tunneling por vías más lentas (UMTS, GPRS, etc.) puede ocurrir que la accesibilidad se indique como negativa aunque, en principio, funcione la comunicación. En este caso, se puede elevar globalmente el tiempo de espera a la respuesta ping (test de accesibilidad).

  Se soporta el establecimiento de una conexión con un MD741-1. En este contexto, se puede configurar una dirección DNS dinámica (vea GETTING STARTED Ejemplo 5: Acceso remoto - ejemplo de túnel VPN con MD741-1 y SOFTNET Security Client (Página 87)).

  Además de los sistemas operativos Windows XP SP2 y Windows XP SP3, también se soporta el sistema operativo Windows 7 (no la versión Home).

- **Datos de configuración para el módulo Modul MD 741-1**

  Para configurar un MD741-1 externo para un acceso con el SOFTNET Security Client V3.0, se pueden extraer datos de configuración a un archivo de texto con el Security Configuration Tool V2.3. (GETTING STARTED Ejemplo 5: Acceso remoto - ejemplo de túnel VPN con MD741-1 y SOFTNET Security Client (Página 87)).

Ámbito de validez de este manual

El presente manual es válido para los siguientes equipos y componentes:

- SIMATIC NET SCALANCE S602 6GK5 602-0BA00-2AA3 - con versión de FW a partir de V2.3
- SIMATIC NET SCALANCE S612 V2 6GK5 612-0BA00-2AA3 - con versión de FW a partir de V2.3
- SIMATIC NET SCALANCE S613 V2 6GK5 613-0BA00-2AA3 - con versión de FW a partir de V2.3
- SIMATIC NET SOFTNET Security Client 6GK1 704-1VW02-0AA0, a partir de la versión 2008
- Security Configuration Tool - versión V2.3

Destinatarios

Este manual está dirigido a personas encargadas de la puesta en servicio del Security Module SCALANCE S así como del SOFTNET Security Client en una red.

Documentación complementaria

En el manual "SIMATIC NET Industrial Ethernet - Redes Twisted Pair y Fiber Optic" se hace referencia a otros productos SIMATIC NET que se pueden utilizar junto con el Security Module SCALANCE S en una red Industrial Ethernet.

Este manual de red se puede obtener en forma electrónica del Customer Support en Internet, descargándolo de la siguiente dirección:

http://support.automation.siemens.com/WW/view/es/1172207
(http://support.automation.siemens.com/WW/view/de/1172207)

Normas y homologaciones

El equipo SCALANCE S cumple los requisitos exigidos para ser provisto de la marca CE. Encontrará información detallada al respecto en el anexo de este manual de instrucciones.

Símbolos utilizados en este manual

Con este símbolo se hace referencia a consejos especiales en estas instrucciones.

El símbolo hace referencia a bibliografía especialmente recomendada.

Este símbolo indica que se puede obtener una ayuda contextual detallada. Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

Referencias bibliográficas /.../

Las referencias a documentación adicional se indican a través de índices bibliográficos escritos entre barras /.../. Por medio de estos números se puede localizar el título de la documentación en la lista de bibliografía que aparece al final del manual.

Contenido

Prólogo **3**

1 Introducción y fundamentos **11**

1.1 Uso de SCALANCE S612, S613 y SOFTNET Security Client 11

1.2 Uso de SCALANCE S602 14

1.3 Configuración y administración 16

2 Propiedades del producto y puesta en servicio **17**

2.1 Propiedades del producto 17
2.1.1 Características de hardware y panorámica de las funciones 17
2.1.2 Volumen de suministro 18
2.1.3 Desembalaje y comprobación 19
2.1.4 Conexión a Ethernet 19
2.1.5 Alimentación eléctrica 20
2.1.6 Contacto de señalización 21
2.1.7 Pulsador Reset - para reponer la configuración al ajuste de fábrica 22
2.1.8 Indicadores 23
2.1.9 Datos técnicos 25

2.2 Montaje 27
2.2.1 Montaje en riel perfil de sombrero 28
2.2.2 Montaje en riel de perfil 30
2.2.3 Montaje mural 30
2.2.4 Puesta a tierra 31

2.3 Puesta en servicio 31
2.3.1 Paso 1: Conectar el módulo SCALANCE S 33
2.3.2 Paso 2: Configurar y cargar 33

2.4 C-PLUG (Configuration-Plug) 35

2.5 Transferir firmware 38

3 GETTING STARTED **39**

3.1 Ejemplo 1: Túnel VPN - Ejemplo de túnel IPsec con SCALANCE S612 / S613 40
3.1.1 Resumen 40
3.1.2 Poner a punto los SCALANCE S y la red 42
3.1.3 Preparar los ajustes de IP de los PCs 43
3.1.4 Crear proyecto y módulos 44
3.1.5 Configurar conexión túnel 46
3.1.6 Cargar la configuración en SCALANCES S 47
3.1.7 Probar la función túnel (Ping-Test) 48

3.2 Ejemplo 2: Firewall - Uso del SCALANCE S como Firewall 50
3.2.1 Resumen 50
3.2.2 Poner a punto los SCALANCE S y la red 52
3.2.3 Preparar los ajustes de IP de los PCs 52
3.2.4 Crear proyecto y módulo 54

3.2.5 Configurar firewall ... 55
3.2.6 Cargar la configuración en SCALANCES S ... 57
3.2.7 Probar la función Firewall (Ping-Test) ... 57
3.2.8 Registro del tráfico de datos del firewall (Logging) ... 59

3.3 Ejemplo 3: Firewall y Router - Uso del SCALANCE S como Firewall y Router ... 60
3.3.1 Resumen ... 60
3.3.2 Poner a punto los SCALANCE S y la red ... 62
3.3.3 Preparar los ajustes de IP de los PCs ... 63
3.3.4 Crear proyecto y módulo ... 65
3.3.5 Configurar modo NAT Router ... 66
3.3.6 Configurar firewall ... 68
3.3.7 Cargar la configuración en SCALANCE S ... 71
3.3.8 Probar la función NAT Router (Ping-Test) ... 71

3.4 Ejemplo 4: Acceso remoto - Ejemplo de túnel VPN con SCALANCE S612 / S613 y SOFTNET Security Client ... 74
3.4.1 Resumen ... 74
3.4.2 Instalar el SCALANCE S y la red ... 76
3.4.3 Preparar ajustes IP de los PCs ... 77
3.4.4 Crear proyecto y módulos ... 79
3.4.5 Configurar conexión túnel ... 82
3.4.6 Cargar la configuración en SCALANCE S y guardar la configuración de SOFTNET Security Client ... 83
3.4.7 Formación de túnel con el SOFTNET Security Client ... 84
3.4.8 Probar la función túnel (Ping-Test) ... 85

3.5 Ejemplo 5: Acceso remoto - ejemplo de túnel VPN con MD741-1 y SOFTNET Security Client ... 87
3.5.1 Sinopsis ... 87
3.5.2 configurar MD741-1 y la red ... 89
3.5.3 Configurar los ajustes de IP de los PCs ... 90
3.5.4 Crear proyecto y módulos. ... 91
3.5.5 Configurar la conexión de túnel ... 93
3.5.6 Guardar la configuración del MD741-1 y del SOFTNET Security Client ... 95
3.5.7 Realizar la configuración del MD741-1 ... 96
3.5.8 Construcción del túnel con el SOFTNET Security Client ... 103
3.5.9 Probar la función del túnel (prueba Ping) ... 105

4 Configuración con Security Configuration Tool ... 107

4.1 Funciones y funcionamiento ... 107

4.2 Instalación ... 109

4.3 Interfaz de usuario y comandos de menú ... 110

4.4 Administración de proyectos ... 113
4.4.1 Resumen ... 113
4.4.2 Creación y edición de proyectos ... 115
4.4.3 Configuración de usuarios ... 118
4.4.4 Check Consistency ... 120
4.4.5 Asignación de nombre simbólicos para direcciones IP o MAC ... 121

4.5 Cargar la configuración en SCALANCES S ... 124

4.6 Datos de configuración para MD 740 / MD 741 ... 126

5 Firewall, Router y otras propiedades del módulo 129

5.1 Vista general / principios 130
5.1.1 SCALANCE S como firewall 130
5.1.2 SCALANCE S como Router 131
5.1.3 SCALANCE S como DHCP-Server 131

5.2 Crear módulos y ajustar parámetros de red 132

5.3 Firewall - Propiedades del módulo en el Standard Mode 135
5.3.1 Configurar firewall 135
5.3.2 Preajuste del firewall 138

5.4 Firewall - Propiedades del módulo en el Advanced Mode 141
5.4.1 Configurar firewall 141
5.4.2 Reglas de Firewall globales 142
5.4.3 Ajuste de reglas de filtros de paquetes IP locales 145
5.4.4 Reglas de filtrado de paquetes IP 147
5.4.5 Definir servicios IP 150
5.4.6 Definir servicios ICMP 152
5.4.7 Ajustar reglas para filtrado de paquetes MAC 154
5.4.8 Reglas para filtrado de paquetes MAC 155
5.4.9 Definir servicios MAC 157
5.4.10 Configurar grupos de servicios 159

5.5 Sincronización horaria 161

5.6 Creación de certificados SSL 163

5.7 Routing Modus 164
5.7.1 Routing 164
5.7.2 Routing NAT/NAPT 165
5.7.3 Routing NAT/NAPT - Ejemplos de configuración, parte 1 170
5.7.4 Routing NAT/NAPT - Ejemplos de configuración, parte 2 172

5.8 Servidor DHCP 174

6 Comunicación segura en la VPN a través de túnel IPsec (S612/S613) 179

6.1 VPN con SCALANCE S 179

6.2 Grupos 183
6.2.1 Crear grupos y asignar módulos 183
6.2.2 Tipos de módulos dentro de un grupo 184

6.3 Configuración de túnel en el Standard Mode 185

6.4 Configuración de túnel en el Advanced Mode 186
6.4.1 Configuración de propiedades de grupo 186
6.4.2 Inclusión del SCALANCE S en un grupo configurado 189
6.4.3 SOFTNET Security Client 190
6.4.4 Configurar propiedades VPN específicas del módulo 191

6.5 Configuración de nodos de red internos 194
6.5.1 Funcionamiento del modo de aprendizaje 195
6.5.2 Visualización de los nodos de red internos encontrados 197
6.5.3 Configuración manual de nodos de red 198

7 SOFTNET Security Client (S612/S613) 201

7.1 Uso de SOFTNET Security Client 201

7.2 Instalación y puesta en servicio del SOFTNET Security Client 204
7.2.1 Instalación e inicio de SOFTNET Security Client 204
7.2.2 Desinstalación de SOFTNET Security Client 205

7.3 Crear un archivo de configuración con la herramienta de configuración Security Configuration Tool 205

7.4 Operación de SOFTNET Security Client 207

7.5 Configuración y edición de túneles 210

8 Funciones online - Test, Diagnóstico y Logging 221

8.1 Panorámica de funciones del cuadro de diálogo online 222

8.2 Registro de eventos (Logging) 224
8.2.1 Log local - ajustes en la configuración 225
8.2.2 Network Syslog - ajustes en la configuración 228
8.2.3 La configuración del Logging de paquetes 231

A Consejos y ayuda 235

A.1 El módulo SCALANCE S no se inicializa correctamente 235

A.2 Módulo SCALANCE S no accesible 235

A.3 Sustitución de un módulo SCALANCE S 235

A.4 El módulo SCALANCE S está comprometido 235

A.5 Clave de los datos de configuración comprometida o perdida 236

A.6 Comportamiento operativo general 237

B Informaciones sobre la identificación CE 239

C Bibliografía 241

D Esquema acotado 243

E Historia del documento 245

E.1 Historia del documento 245

Glosario / lista de abreviaturas 247

Índice alfabético 259

Introducción y fundamentos

1

Con SIMATIC NET SCALANCE S y SIMATIC NET SOFTNET Security Client se ha decidido por el concepto de seguridad SIEMENS, que satisface los altos requisitos exigidos a la seguridad de la comunicación en la técnica de automatización industrial.

Este capítulo le proporciona una visión de conjunto de las funciones de seguridad propias de los equipos y los componentes

- Security Module SCALANCE S
- SOFTNET Security Client

Un consejo:
Encontrará una descripción del acceso rápido con SCALANCE S en el capítulo 3 "GETTING STARTED".

1.1 Uso de SCALANCE S612, S613 y SOFTNET Security Client

Protección completa - misión de SCALANCE S612 / S613

Por combinación de diversas medidas de seguridad, como son Firewall, router NAT/NAPT y VPN (Virtual Private Network) a través de túnel IPsec, los SCALANCE S612 / S613 protegen equipos concretos o también células de automatización completas de:

- Espionaje de datos
- Manipulación de datos
- Accesos no autorizados

SCALANCE S612 / S613 hace posible una protección flexible, exenta de retroacciones, independiente de protocolos (a partir de Layer 2 según IEEE 802.3) y con un manejo sin complicaciones.

SCALANCE S612 / S613 y SOFTNET Security Client se configuran con la herramienta Security Configuration Tool.

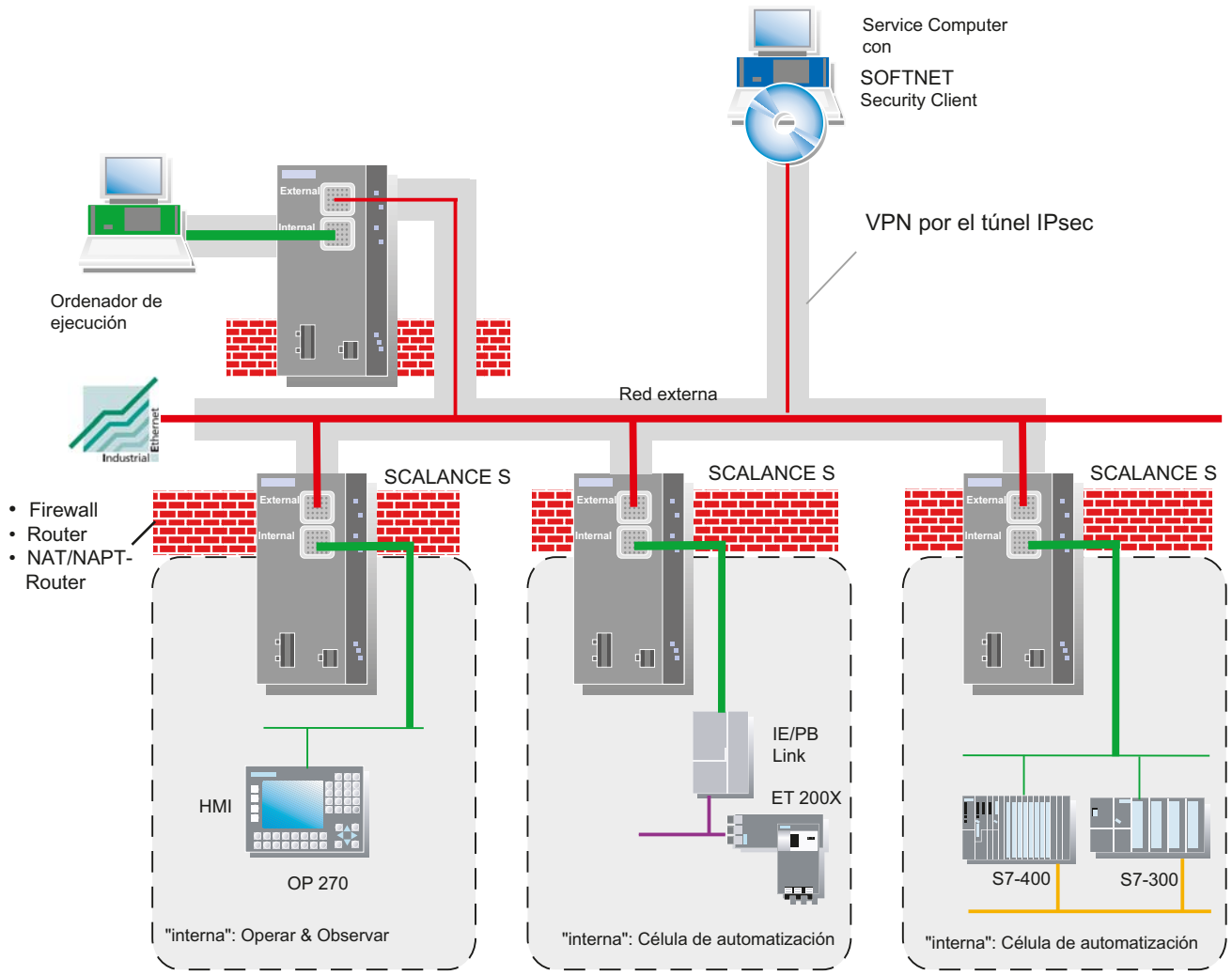


Figura 1-1 Configuración de red con SCALANCE S612 / S613

Funciones de seguridad

- Firewall
  - IP-Firewall con Stateful Packet Inspection;
  - Firewall también para telegramas Ethernet-"Non-IP" según IEEE 802.3 (telegramas Layer 2; no es válido si se usa el modo de router)
  - Limitación del ancho de banda

  Todos los nodos de red que se encuentran en el segmento de red interno de un SCALANCE S son protegidos por su firewall.
- Comunicación protegida por túnel IPsec

  SCALANCE S612 / S613 y SOFTNET Security Clients se pueden reunir en grupos a través de la configuración. Entre todos los SCALANCE S612 / S613 y un SOFTNET Security Client de un grupo se establecen túneles IPsec (VPN, Virtual Private Network). Todos los nodos internos de estos SCALANCE S se pueden comunicar entre sí por estos túneles de forma protegida.
- Independencia de protocolo

  El establecimiento de túneles comprende también telegramas Ethernet según IEEE 802.3 (telegramas Layer 2; no es válido si se usa el modo de router)

  A través de los túneles IPsec se transmiten tanto telegramas IP como también No-IP.
- Modo Router

  Utilizando SCALANCE S como router conecta la red interna con la red externa. La red interna conectada a través de SCALANCE S se convierte así en una subred propia.
- Protección para equipos y segmentos de red

  La función de protección de Firewall y VPN se puede extender al uso de equipos concretos, de varios equipos o también de segmentos de red enteros.
- Ausencia de retroacciones en caso de instalación en redes planas (modo Bridge)

  Nodos de red internos se pueden localizar sin configuración. Por lo tanto, al montar un SCALANCE S612 / S613 en una infraestructura de red ya existente no se necesita configurar de nuevo los equipos terminales.

  El módulo intenta encontrar estaciones internas; sin embargo se tienen que configurar las estaciones internas que no se localicen por este procedimento.

Comunicación con PC/PG en la tarea VPN del SOFTNET Security Client

Con el software de PC SOFTNET Security Client son posibles accesos remotos del PC/PG a equipos de automatización protegidos por SCALANCE S, más allá de los límites de redes públicas.

Mediante el SOFTNET Security Client se configura automáticamente un PC/PG de manera que pueda establecer con uno o varios SCALANCE S una comunicación túnel IPsec protegida en la VPN (Virtual Private Network).

Aplicaciones de PG/PC, como por ejemplo Diagnóstico NCM o STEP7, pueden acceder así a través de una conexión túnel protegida a equipos o redes que se encuentren en una red interna protegida por SCALANCE S.

El software de PC SOFTNET Security Client se configura también con la herramienta de configuración Security Configuration Tool; esto garantiza una configuración coherente que no necesita conocimientos de seguridad especiales.

Nodos de red internos y externos

SCALANCE S612 / S613 divide las redes en dos áreas:

- Red interna: áreas protegidas con los "nodos internos"

  Nodos internos son todos aquellos nodos protegidos por un SCALANCE S.

- Red externa: áreas no protegidas con los "nodos externos"

  Nodos externos son todos los nodos que se encuentran fuera de las áreas protegidas.

ATENCIÓN
Las redes internas se consideran seguras (dignas de confianza). Conecte un segmento de red interno con los segmentos de red externos sólo a través de SCALANCE S. ¡No deben existir otras vías de conexión entre la red interna y la externa!

1.2 Uso de SCALANCE S602

Firewall y Router - misión de SCALANCE S602

Por combinación de diversas medidas de seguridad, como son Firewall y Router NAT/NAPT, el SCALANCE S602 protege equipos concretos o también células de automatización completas de:

- Espionaje de datos
- Accesos no autorizados

SCALANCE S602 hace posible esta protección de forma flexible y con un manejo sin complicaciones.

SCALANCE S602 se configura con la herramienta de configuración Security Configuration Tool.

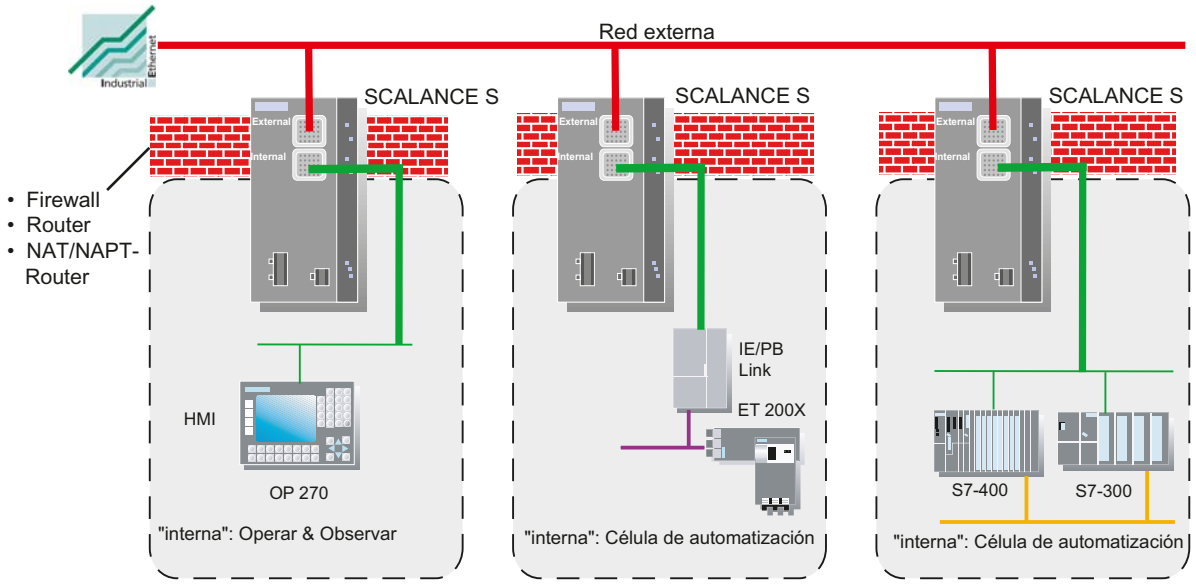


Figura 1-2 Configuración de red con SCALANCE S602

Funciones de seguridad

- Firewall
  - IP-Firewall con Stateful Packet Inspection;
  - Firewall también para telegramas Ethernet-"Non-IP" según IEEE 802.3 (telegramas Layer 2; no es válido para S602 si se utiliza el modo Router);
  - Limitación del ancho de banda

  Todos los nodos de red que se encuentran en el segmento de red interno de un SCALANCE S son protegidos por su firewall.
- Modo Router

  Utilizando SCALANCE S como router desacopla la red interna de la red externa. La red interna conectada por el SCALANCE S se convierte así en una subred propia; el SCALANCE S se tiene que direccionar como Router explícitamente a través de su dirección IP.
- Protección para equipos y segmentos de red

  La función de protección de Firewall se puede extender al uso de equipos concretos, de varios equipos o también de segmentos de red enteros.
- Ausencia de retroacciones en caso de instalación en redes planas (modo Bridge)

  Por lo tanto, al montar un SCALANCE S602 en una infraestructura de red ya existente no se necesita ajustar de nuevo los equipos terminales.

Nodos de red internos y externos

SCALANCE S602 divide las redes en dos áreas:

- Red interna: áreas protegidas con los "nodos internos"

  Nodos internos son todos aquellos nodos protegidos por un SCALANCE S.

- Red externa: áreas no protegidas con los "nodos externos"

  Nodos externos son todos los nodos que se encuentran fuera de las áreas protegidas.

ATENCIÓN
Las redes internas se consideran seguras (dignas de confianza). Conecte un segmento de red interno con los segmentos de red externos sólo a través de SCALANCE S. ¡No deben existir otras vías de conexión entre la red interna y la externa!

1.3 Configuración y administración

Lo más importante, en resumen

En combinación con la herramienta de configuración Security Configuration Tool se logra una aplicación sencilla y segura de los módulos SCALANCE S:

- Configuración sin conocimientos de experto en materia de IT con la Security Configuration Tool

  Con la Security Configuration Tool pueden ajustar un módulo SCALANCE S incluso personas que no sean expertas en materia de IT. En un modo extendido se pueden realizar ajustes más complejos, si ello es necesario.

- Comunicación administrativa segura

  La transmisión de los ajustes se efectúa en el SCALANCE S a través de una conexión con codificación SSL.

- Protección de acceso en la Security Configuration Tool

  La administración de usuarios de la Security Configuration Tool garantiza una protección de acceso para los equipos SCALANCE S y los datos de configuración.

- Medio intercambiable C-PLUG

  El C-PLUG es un medio intercambiable, enchufable, en el que están almacenados datos de configuración en forma codificada. Si se sustituye un SCALANCE S, gracias a él se puede realizar la configuración sin necesidad de PC/PG.

Propiedades del producto y puesta en servicio 2

Este capítulo le familiarizará con el manejo y todas las propiedades importantes del equipo SCALANCE S.

En él se informa sobre qué posibilidades de montaje existen y sobre cómo se pone el equipo en funcionamiento con unas pocas operaciones.

Otras informaciones

La configuración del equipo para aplicaciones estándar se describe de forma resumida en el capítulo "GETTING STARTED".

Encontrará detalles sobre la configuración y las funciones online en la parte de consulta de este manual.

2.1 Propiedades del producto

Nota

Las homologaciones o autorizaciones indicadas sólo se consideran otorgadas si el producto está provisto del correspondiente distintivo.

2.1.1 Características de hardware y panorámica de las funciones

Todos los módulos SCALANCE S ofrecen las siguientes prestaciones fundamentales:

Hardware

- carcasa robusta con grado de protección IP 30
- opcionalmente, montaje sobre riel de perfil de sombrero S7-300 o DIN de 35 mm
- alimentación de tensión redundante

- contacto de señalización
- gama de temperatura ampliada (-20 °C a +70 °C SCALANCE S613)

Panorámica de funciones de los tipos de equipos

Vea en la tabla siguiente a qué funciones se da soporte en su equipo.

Nota

En este manual se describen todas las funciones. Al utilizar la siguiente tabla, tenga en cuenta qué descripciones corresponden al equipo utilizado por usted.

Preste también atención a los datos adicionales que aparecen en los títulos de los capítulos.

Tabla 2- 1 Panorámica de funciones

Función	S602	S612 V1	S612 V2	S613 V1	S613 V2
Firewall	X	X	X	X	X
Router NAT/NAPT	X	-	X	-	X
Servidor DHCP	X	-	X	-	X
Syslog de red	X	-	X	-	X
Túnel IPsec (VPN, Virtual Private Network).	-	X	X	X	X
SOFTNET Security Client	-	X	X	X	X

Se soporta a la función **x**

- No se soporta la función

2.1.2 Volumen de suministro

¿Qué se entrega con el SCALANCE S?

- Equipo SCALANCE S
- Bloque de bornes enchufable, de 2 polos

- Bloque de bornes enchufable, de 4 polos
- Informaciones sobre el producto Produkt
- CD con el siguiente contenido:
  - manual
  - software de configuración Security Configuration Tool

2.1.3 Desembalaje y comprobación

Desembalar, comprobar

1. Compruebe la integridad del suministro.
2. Examinar todas las piezas para ver si han sufrido daños durante el transporte.

⚠ ADVERTENCIA
Sólo se deben poner en funcionamiento piezas intactas.

2.1.4 Conexión a Ethernet

Posibilidades de conexión

El SCALANCE S cuenta con 2 conectores hembra RJ-45 para la conexión a Ethernet.

Nota

En el puerto TP en ejecución RJ–45 se pueden conectar cables TP o cables TP-XP de una longitud máxima de 10 m.

En combinación con el Industrial Ethernet FastConnect IE FC Standard Cable y el IE FC RJ–45 Plug 180 se permite una longitud total de cable de como máximo 100 m entre dos equipos.

ATENCIÓN

Las conexiones de Ethernet en Port 1 y Port 2 son tratadas de forma diferente por el SCALANCE S, por lo que no se deben confundir al establecer la conexión con la red de comunicación:

- Port 1 - External Network
  conector hembra RJ–45 superior, marca roja = área de red no protegida;
- Port 2 - Internal Network
  conector hembra RJ45 inferior, marca verde = red protegida por SCALANCE S;

Si se permutan los puertos, el equipo pierde su función de protección.

Autonegotiation

SCALANCE S soporta Autonegotiation.

Por Autonegotiation se entiende que los parámetros de conexión y transmisión son negociados automáticamente con el nodo de red interrogado.

Función MDI /MDIX Autocrossing

SCALANCE S soporta la función MDI / MDIX Autocrossing.

La función MDI /MDIX Autocrossing ofrece la ventaja de un cableado continuo, sin que se requieran cables Ethernet externos, cruzados. Con esto se evitan funciones incorrectas por confusión de los cables de emisión y recepción. La instalación se simplifica así notablemente.

2.1.5 Alimentación eléctrica

⚠ ADVERTENCIA

El equipo SCALANCE S está previsto para funcionar con baja tensión de seguridad. En consecuencia, a las conexiones de alimentación sólo se deben conectar bajas tensiones de seguridad (SELV) según IEC950/EN60950/ VDE0805.

La fuente de alimentación utilizada para el SCALANCE S tiene que ser del tipo NEC Class 2 (gama de tensión 18-32 V, consumo de corriente 250 mA).

El equipo se debe abastecer únicamente con una unidad de alimentación eléctrica que cumpla los requisitos de la clase 2 para alimentaciones eléctricas según "National Electrical Code, table 11 (b)". En caso de estructura con alimentación eléctrica redundante, es decir, con dos dispositivos de alimentación eléctrica separados, ambos tienen que cumplir estos requisitos.

ATENCIÓN
No conecte nunca el SCALANCE S a tensión alterna o a tensiones continuas de más de 32 V DC.

La alimentación eléctrica se conecta a través de un bloque de bornes enchufable de 4 polos. La alimentación eléctrica se puede conectar de forma redundante. Ambas entradas están desacopladas. No existe distribución de carga. En el caso de alimentación redundante, la fuente de alimentación con la tensión de salida más alta abastece ella sola al SCALANCE S. La alimentación eléctrica está conectada a la carcasa con impedancia elevada, lo que permite un montaje sin puesta a tierra.

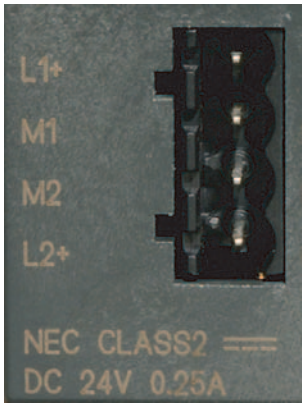


Figura 2-1 Alimentación eléctrica

2.1.6 Contacto de señalización

ATENCIÓN
El contacto de señalización se debe someter a una carga máxima de 100 mA (tensión de seguridad (SELV), DC 24 V). No conecte nunca el SCALANCE S a tensión alterna o a tensiones continuas de más de 32 V DC.

El contacto de señalización se conecta a través de un bloque de bornes enchufable de 2 polos. El contacto de señalización es un interruptor sin potencial con el que se notifican estados de error a través de una interrupción del contacto.

A través del contacto de señalización se pueden señalizar los siguientes errores o defectos:

- Fallos en la alimentación eléctrica
- Fallos internos

En caso de fallo o si el SCALANCE S está sin tensión, está abierto el contacto de señalización. En caso de funcionamiento sin fallos, está cerrado.

Figura 2-2 Contacto de señalización

2.1.7 Pulsador Reset - para reponer la configuración al ajuste de fábrica

SCALANCE S tiene un pulsador de Reset. El pulsador Reset se encuentra en la parte posterior de la carcasa, debajo de la tapa roscada, directamente junto al C-PLUG.

El pulsador Reset está protegido mecánicamente contra un accionamiento no intencionado.

ATENCIÓN
Asegúrese de que sólo personal autorizado tenga acceso al SCALANCE S.

¿Qué función tiene el pulsador?

Con el pulsador Reset se pueden activar dos funciones:

- Reinicio

  El módulo arranca de nuevo. La configuración cargada se conserva.

- Reposición a la configuración de fábrica

  El módulo arranca de nuevo y se repone al estado que tenía a la entrega. Una configuración cargada se borra.

Reinicio - Proceda del siguiente modo

1. Si es necesario, desmonte el módulo SCALANCE S para acceder a la cavidad.
2. Quite el tapón M32 de la parte posterior del equipo.

   En pulsador Reset están alojado en una cavidad en la parte posterior del SCALANCE S, directamente junto a la ranura para el C-PLUG. Esta cavidad está protegida por un tapón de rosca. El pulsador se encuentra en un orificio de pequeño diámetro, estando así protegido de un accionamiento por descuido.

3. Presione el pulsador Reset durante menos de 5 segundos.

   El proceso de reinicio dura hasta 2 minutos. Durante el proceso de reinicio está encendido el indicador Fault con luz amarilla. Cuide de que durante ese tiempo no se interrumpa la alimentación eléctrica.

   Una vez finalizado el reinicio, el equipo pasa automáticamente al modo productivo. El indicador Fault brilla entonces con luz verde constante.

4. Cierre la cavidad con el tapón M32 y monte el equipo.

Reposición a la configuración de fábrica - Proceda del siguiente modo

ATENCIÓN
Si al restablecer la configuración de fábrica está conectado un C-PLUG, se borra el contenido del C-PLUG.

1. Si es necesario, desmonte el módulo SCALANCE S para acceder a la cavidad.
2. Quite el tapón M32 de la parte posterior del equipo.

   En pulsador Reset están alojado en una cavidad en la parte posterior del SCALANCE S, directamente junto a la ranura para el C-PLUG. Esta cavidad está protegida por un tapón de rosca. El pulsador se encuentra en un orificio de pequeño diámetro, estando así protegido de un accionamiento por descuido.

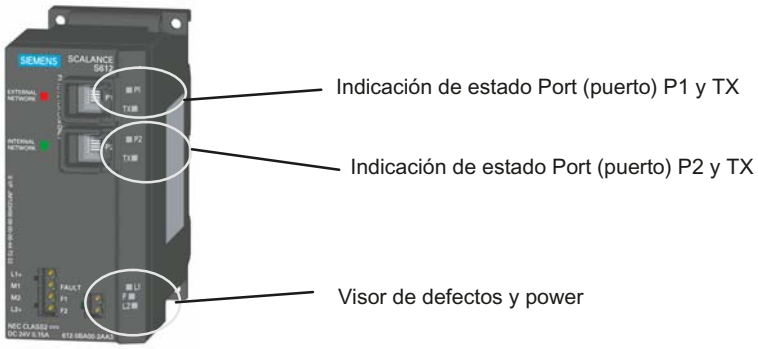
3. Presione el pulsador Reset y manténgalo apretado (durante más de 5 segundos) hasta que destelle con luz amarilla-roja el indicador Fault.

   El proceso de reposición dura hasta 2 minutos. Durante el proceso de reposición parpadea el indicador Fault con luz amarilla-roja. Cuide de que durante ese tiempo no se interrumpa la alimentación eléctrica.

   Una vez terminado el proceso de reposición, el equipo rearranca automáticamente. El indicador Fault brilla entonces con luz amarila constante.

4. Cierre la cavidad con el tapón M32 y monte el equipo.

2.1.8 Indicadores



Indicador de error (Fault LED)

Indicación del estado operativo:

Estado	Significado
luz roja	El módulo detecta un fallo. (El contacto de señalización está abierto) Se identifican los siguientes errores o defectos: • Fallo interno (por ejemplo: arranque fracasado) • C-PLUG no válido (formateado no válido)
luz verde	El módulo está en servicio productivo (El contacto de señalización está cerrado).
apagado	El módulo ha fallado; no hay alimentación eléctrica (El contacto de señalización está abierto).
luz amarilla (continua)	El módulo está en la fase de arranque (El contacto de señalización está abierto). Si no existe dirección IP, el módulo permanece en este estado.
destella alternadamente con luz amarilla-roja	El módulo se repone al estado que tenía a la entrega. (El contacto de señalización está abierto).

Indicador Power (L1, L2)

El estado de la alimentación eléctrica es señalizado por dos LEDs:

Estado	Significado
luz verde	Está conectada la alimentación eléctrica L1 o L2.
apagado	La alimentación eléctrica L1 o L2 no está conectada o es <14 V (L+)
luz roja	La alimentación eléctrica L1 o L2 ha fallado durante el servicio o es <14 V (L+)

Indicadores de estado de puerto (P1 y TX, P2 y TX)

El estado de los puertos es señalizado por respectivamente dos 2 LEDs para las dos conexiones:

Estado	Significado
LED P1 / P2	
luz verde	TP-Link presente
destella / brilla con luz amarilla	Recepción de datos en RX
apagado	No hay TP-Link o no se reciben datos
LED TX	
destella / brilla con luz amarilla	Se envían datos
apagado	No se envían datos

2.1.9 Datos técnicos

Conexiones	
Conexión de equipos terminales o componentes de red a través de Twisted Pair	2 conectores hembra RJ–45 con asignación MDI-X 10/100 Mbit/s (semidúplex/dúplex completo)
Conexión de la alimentación eléctrica	1 bloque de bornes enchufable, de 4 polos
Conexión para contacto de señalización	1 bloque de bornes enchufable, de 2 polos
Datos eléctricos	
Tensión de alimentación	Alimentación DC 24 V (DC 18 hasta 32 V) • de ejecución redundante • Baja tensión de seguridad (SELV)
Potencia perdida para DC 24 V	3,84 W
Consumo de corriente con la tensión nominal	250 mA como máximo
Longitudes de cables permitidas	
Conexión a través de cables Industrial Ethernet FC TP:	
0 - 100 m	Industrial Ethernet FC TP Standard Cable con IE FC RJ–45 Plug 180 o a través de Industrial Ethernet FC Outlet RJ–45 con 0 - 90 m Industrial Ethernet FC TP Standard Cable + 10 m TP Cord
0 - 85 m	Industrial Ethernet FC TP Marine/Trailing Cable con IE FC RJ–45 Plug 180 o 0 - 75 m Industrial Ethernet FC TP Marine/Trailing Cable + 10 m TP Cord
Recursos de software para VPN	
Cantidad de túneles IPsec	
SCALANCE S612	64 como máximo
SCALANCE S613	128 como máximo
Recursos de software "Firewall"	
Cantidad de bloques de reglas de Firewall	
SCALANCE S602	256 como máximo
SCALANCE S612	256 como máximo
SCALANCE S613	256 como máximo
Condiciones ambientales permitidas / compatibilidad electromagnética	
Temperatura de funcionamiento SCALANCE S602	0 °C a +60 °C
Temperatura de funcionamiento SCALANCE S612	0 °C a +60 °C
Temperatura de funcionamiento SCALANCE S613	-20 °C a +70 °C
Temperatura de almacén/transporte	-40 °C a +80 °C

Humedad relativa en funcionamiento	95 % (sin condensación)
Altura en funcionamiento	hasta 2000 m sobre el nivel del mar con máx. 56 °C de temperatura ambiente hasta 3000 m sobre el nivel del mar con máx. 50 °C de temperatura ambiente
Grado de radiointerferencias	EN 50081-2 Class A
Inmunidad a interferencias	EN 50082-2
Grado de protección	IP 30
Homologaciones	
c-UL-us	UL 60950
	CSA C22.2 Nr. 60950
c-Ul-us for Hazardous Locations	UL 1604, UL 2279Pt.15
FM	FM 3611
C-TICK	AS/NZS 2064 (Class A).
CE	EN 50081-2, EN 50082-2
ATEX Zona 2	EN50021
MTBF	81,09 años
Construcción	
Medidas (An x Al x Prof) en mm	60 x 125 x 124
Peso en g	780
Posibilidades de montaje	• Riel perfil de sombrero • Riel de perfil S7-300 • Montaje mural
Referencias de pedido	
SCALANCE S602	6GK5602-0BA00-2AA3
SCALANCE S612	6GK5612-0BA00-2AA3
SCALANCE S613	6GK5613-0BA00-2AA3
Manual "Industrial Ethernet - Redes TP y Fiber Optic"	6GK1970-1BA10-0AA0
Números de referencia para accesorios	
IE FC Stripping Tool	6GK1901-1GA00
IE FC Blade Cassettes	6GK1901-1GB00
IE FC TP Standard Cable	6XV1840 2AH10
IE FC TP Trailing Cable	6XV1840-3AH10
IE FC TP Marine Cable	6XV1840-4AH10
IE FC RJ–45 Plug 180 unidad de embalaje = 1 pieza	6GK1 901-1BB10-2AA0
IE FC RJ–45 Plug 180 unidad de embalaje = 10 piezas	6GK1 901-1BB10-2AB0
IE FC RJ–45 Plug 180 unidad de embalaje = 50 piezas	6GK1 901-1BB10-2AE0

2.2 Montaje

Nota

Los requisitos de la norma EN61000-4-5, Comprobación de fuentes en líneas de alimentación eléctrica, sólo se cumplen si se utiliza un descargador de corrientes de rayo Blitzductor VT AD 24V Ref. 918 402.

Fabricante:
DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str.1, Postfach 1640, D-92306 Neumarkt / Alemania

⚠ ADVERTENCIA

Para uso en condiciones de protección contra explosión (Zona 2), el producto SCALANCE S se tiene que montar en una carcasa.

En el ámbito de validez de ATEX 95 (EN 50021), esta carcasa ha de ser conforme al menos con IP54 según EN 60529.

ADVERTENCIA
EL EQUIPO SÓLO SE DEBE CONECTAR A / DESCONECTAR DE LA ALIMENTACIÓN ELÉCTRICA SI SE PUEDE EXCLUIR CON TODA SEGURIDAD LA EXISTENCIA DE UN RIESGO DE EXPLOSIÓN.

Tipos de montaje

El SCALANCE S permite varias formas de montaje:

- Montaje en riel perfil de sombrero DIN de 35 mm
- Montaje en un riel de perfil SIMATIC S7-300
- Montaje mural

Nota

Para la instalación y el uso, tenga en cuenta las directivas de montaje y las consignas de seguridad que aparecen en esta descripción así como en el manual SIMATIC NET Industrial Ethernet - Redes Twisted Pair y Fiber Optic /1/.

ATENCIÓN

Se recomienda proteger el equipo de los rayos solares directos con un objeto dispensador de sombra apropiado.

Esto evita un calentamiento no deseado del equipo y evita un envejecimiento prematuro tanto del equipo como del cableado.

2.2.1 Montaje en riel perfil de sombrero

Montaje

Monte el SCALANCE S sobre un riel de perfil de sombrero de 35 mm según DIN EN 50022.

1. Enganche la guía de fijación superior del equipo en el riel perfil de sombrero y presiónela hacia abajo contra dicho riel hasta que se encastre.
2. Monte los cables de conexión eléctrica y el bloque de bornes para el contacto de señalización.

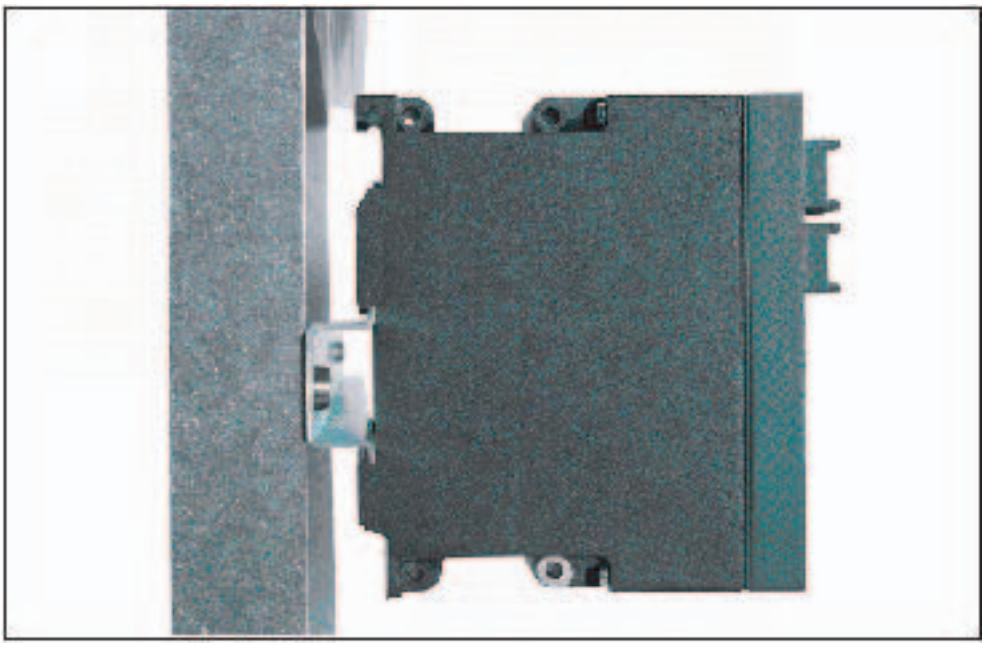


Figura 2-3 SCALANCE S - Montaje en un riel perfil de sombrero DIN (35mm)

Desmontaje

Para retirar el SCALANCE S del riel perfil de sombrero:

1. Desmonte primero los cables TP y desenchufe el bloque de bornes para la alimentación eléctrica y el contacto de señalización.

2. Desenclave con un destornillador el encastre del riel perfil de sombrero en la parte inferior del equipo y separe luego del riel perfil de sombrero la parte de abajo del equipo.

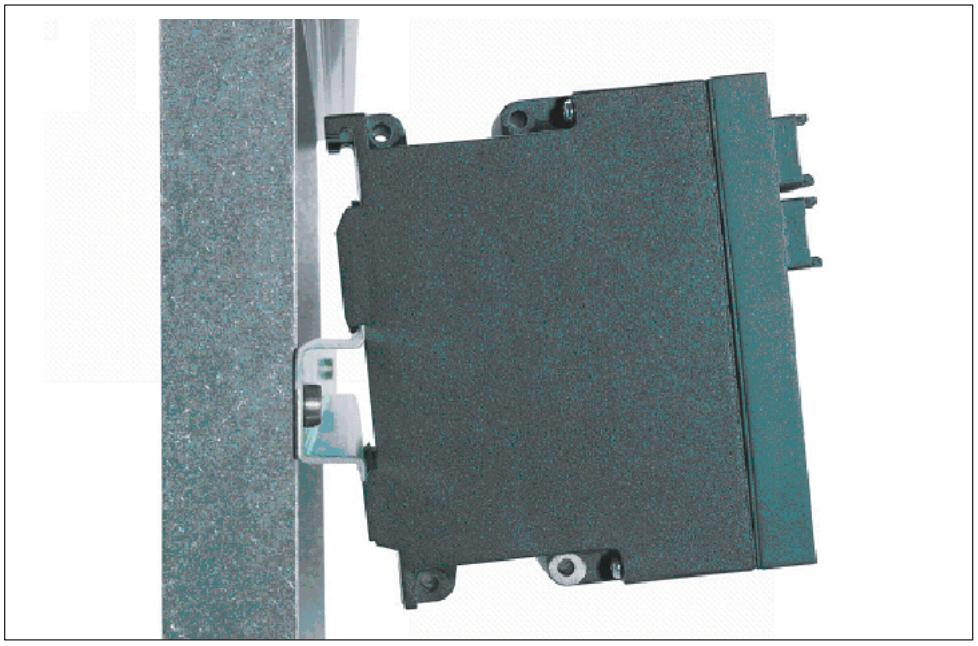


Figura 2-4 SCALANCE S - Desmontaje de un riel perfil de sombrero DIN (35mm)

2.2.2 Montaje en riel de perfil

Montaje en un riel de perfil SIMATIC S7-300

1. Enganche la guía de la parte superior de la carcasa del SCALANCE S en el riel de perfil S7.
2. Atornille el equipo SCALANCE S en la parte inferior del riel de perfil.

Figura 2-5 SCALANCE S - Montaje en un riel de perfil SIMATIC S7-300

2.2.3 Montaje mural

Material de montaje

Utilice para la fijación, por ejemplo a una pared de hormigón:

- 4 tacos para pared de 6 mm de diámetro y 30 mm de longitud;
- tornillos de 3,5 mm de diámetro y 40 mm de longitud.

Nota

La fijación a la pared debe estar concebida de forma que pueda soportar al menos un peso cuádruple del peso propio del equipo.

2.2.4 Puesta a tierra

Montaje en riel perfil de sombrero

La puesta a tierra se realiza a través del riel perfil de sombrero.

Riel de perfil S7

La puesta a tierra tiene lugar a través de la parte posterior del aparato y del tornillo de gollete.

Montaje mural

La puesta a tierra se realiza con el tornillo de fijación a través del orificio exento de pintura o barniz.

ATENCIÓN
Tenga en cuenta que el SCALANCE S se tiene que poner a tierra con una ohmicidad lo más baja posible.

2.3 Puesta en servicio

ATENCIÓN
Antes de la puesta en servicio, lea con atención las informaciones de los capítulos "Propiedades del producto" y "Montaje" y siga especialmente las instrucciones de seguridad.

Principio

Para trabajar con un SCALANCE S se tiene que cargar una configuración realizada con la Security Configuration Tool. A continuación se describe este procedimiento.

La configuración de un SCALANCE S abarca los parámetros IP y el ajuste de reglas de firewall así como, si procede, el ajuste de túneles IPsec (S612 / S613) o del modo Router.

Básicamente, antes de la configuración se puede realizar primero offline la configuración completa, cargándola a continuación. Para la primera configuración (ajustes de fábrica) debe utilizar para el direccionamiento la dirección MAC impresa sobre el equipo.

Según la aplicación, al realizar la puesta en servicio se carga la configuración en uno o en varios módulos simultáneamente.

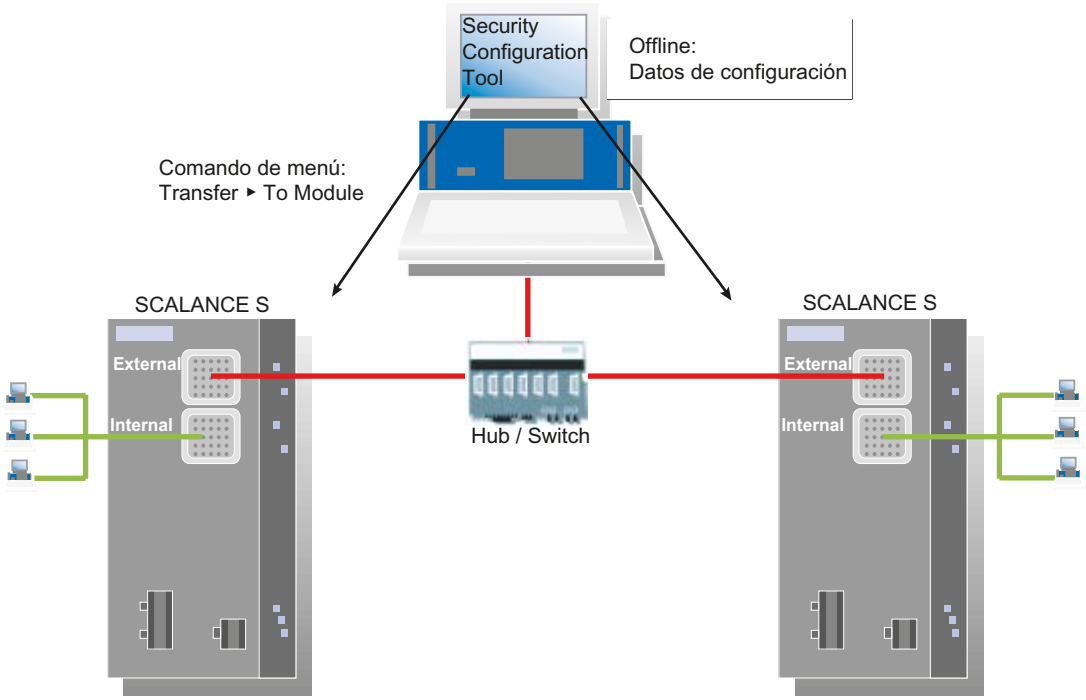


Figura 2-6 Gráfica general Puesta en servicio

Configuración de fábrica

Con la configuración de fábrica (estado a la entrega o tras "reposición a la configuración de fábrica"), el SCALANCE S presenta el siguiente comportamiento tras conectar la tensión de alimentación:

- No es posible la comunicación IP, ya que faltan los ajustes IP; en especial el SCALANCE S no tiene todavía dirección IP.

  En cuanto se ha asignado al módulo SCALANCE S una dirección IP válida por configuración, se puede acceder también al módulo a través de Router (entonces es posible la comunicación IP).
- El equipo tiene una dirección MAC preajustada fija; la dirección MAC está empresa en el equipo y se tiene que introducir para la configuración.
- El firewall está preconfigurado con las siguientes reglas de firewall:
  - el tráfico de datos no asegurado del puerto interno al puerto externo y viceversa (externo ↔ interno) **no** es posible;

El estado no configurado se reconoce porque el diodo F brilla con luz amarilla.

Consulte también

Propiedades del producto (Página 17)
Montaje (Página 27)

2.3.1 Paso 1: Conectar el módulo SCALANCE S

Proceda del siguiente modo:

1. Saque primero el SCALANCE S de su embalaje y compruebe si está en perfecto estado.
2. Conecte la alimentación de tensión a SCALANCE S.

   Resultado: Tras conectar la tensión de servicio brilla el diodo Fault (F) con luz amarilla.
3. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45).

   Conecte el puerto 1 (puerto externo) a la red externa en la que está conectado el PC/PG de configuración.

   Conecte el puerto 2 (puerto interno) a la red interna.

   Observación:
   A la puesta en servicio puede conectar, por principio, el PC/PG de configuración primero al puerto 1 o al puerto 2, renunciando a la conexión de otros nodos de red hasta que el equipo esté provisto de una configuración. En caso de conexión al puerto 2 debería configurar, sin embargo, cada módulo SCALANCE S por separado.
4. Continúe con el siguiente paso "Configurar y cargar".

2.3.2 Paso 2: Configurar y cargar

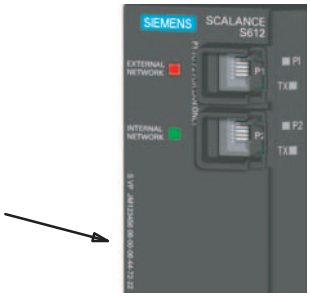
A continuación se describe cómo se configura el módulo SCALANCE S partiendo de los ajustes de fábrica.

Proceda del siguiente modo:

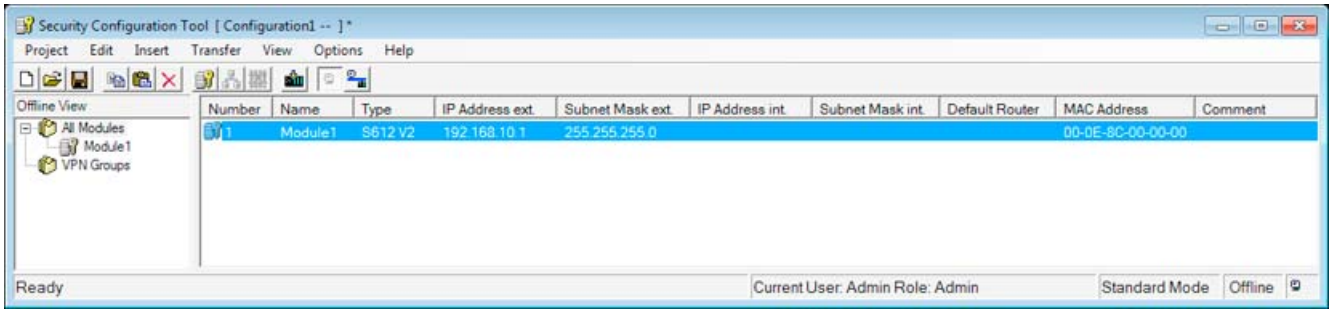
1. Inicie la herramienta de configuración Security Configuration Tool adjuntada.
2. Seleccione el comando de menú **Project ▸ New.**

   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted entra aquí se le asigna el papel de un administrador.
3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto crea un nuevo proyecto.
4. Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software". Configure ahora su tipo de producto, el módulo y la versión de firmware.

5. Introduzca en el campo de la "Dirección MAC" en el área de "Configuración" la dirección MAC impresa en la carcasa del módulo en el formato especificado.
   Podrá encontrar esta dirección en la página principal del módulo SCALANCE S (véase la figura).



6. Introduzca la dirección IP externa y la máscara de subred externa en el área "Configuración", dentro de los campos previstos para ello, y confirme el diálogo con "OK". De ahí en adelante se incluirá su módulo en la lista de los módulos configurados.
7. Seleccione su módulo e introduzca la dirección IP del Default Router haciendo clic en la columna señalada como "Default Router".


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 00-0E-8C-00-00-00
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

   opcional: Configure eventualmente otras propiedades del módulo y de los grupos de módulos.

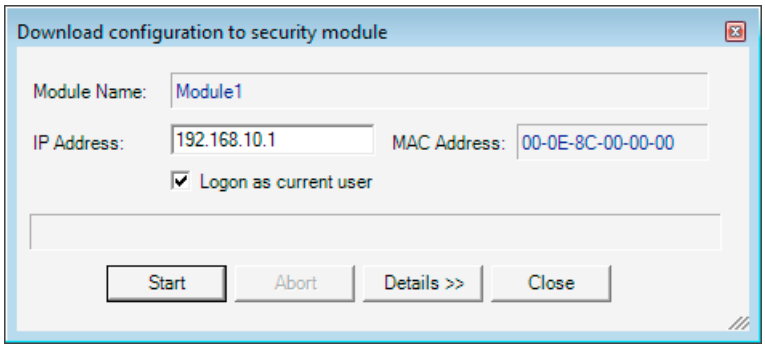
8. Guarde ahora el proyecto con el siguiente comando de menú, bajo un nombre apropiado:

   Project ▸ Save As…

9. Seleccione el siguiente comando de menú:

   Transfer ▸ To Module...

   Aparece el siguiente cuadro de diálogo de transferencia:



10. Haciendo clic en el botón "Start" se transfiere la configuración al módulo SCALANCE S.

    Resultado: El módulo SCALANCE S está ahora configurado y se puede comunicar a nivel de IP. Este estado es señalizado por el diodo indicador Fault con luz verde.

2.4 C-PLUG (Configuration-Plug)

Aplicaciones

El C-PLUG es un medio intercambiable para salvaguardia de datos de configuración del equipo básico (SCALANCE S). De este modo, los datos de configuración siguen estando disponibles aunque se cambie el equipo básico.

Principio de funcionamiento

El suministro de energía corre a cargo del equipo básico. El C-PLUG conserva todos los datos de modo permanente, aún sin estar conectado a la alimentación de corriente.

Colocación en el lugar de enchufe del C-PLUG

El lugar de enchufe para el C-PLUG se encuentra en la parte posterior del equipo. Proceda del siguiente modo para colocar el C-PLUG:

1. Quite la tapa roscada M32.

2. Introduzca el C-PLUG en el compartimento previsto al efecto.
3. Cierre a continuación el compartimento con la tapa roscada M32.

ATENCIÓN
Observe el estado operativo
¡Enchufar y desenchufar el C-PLUG únicamente en estado sin tensión!

Figura 2-7 Colocar el C-PLUG en el equipo y sacar el C-PLUG del equipo con ayuda de un destornillador.

Función

En un C-PLUG no escrito (estado de fábrica) se salvan automáticamente todos los datos de configuración del SCALANCE S al arrancar el equipo. Igualmente se salvan en el C-PLUG todas las modificaciones introducidas en la configuración durante el funcionamiento del equipo, sin que ello requiera una intervención del operador.

Un equipo básico con C-PLUG enchufado utiliza automáticamente para el arranque los datos de configuración disponibles en dicho C-PLUG enchufado. Condición para ello es que los datos hayan sido escritos por un tipo de equipo compatible.

De este modo, en caso de avería se puede sustituir el equipo básico de forma sencilla y rápida. En caso de sustitución se toma el C-PLUG del componente averiado y se enchufa en el componente de recambio. Después del primer arranque, el equipo sustituto tiene automáticamente la misma configuración que el equipo que había fallado.

Nota

Datos de configuración coherentes - Adaptar dirección MAC

Después de sustituir el equipo por uno de recambio, los datos de configuración deberían ser en conjunto coherentes. Para ello debería adaptar en la configuración la dirección MAC a la dirección MAC impresa en la carcasa del equipo de recambio.

Si utiliza en el equipo de recambio la C-PLUG ya configurado del equipo sustituido, esta medida no es sin embargo imprescindible para el arranque y el uso del equipo.

ATENCIÓN
Reposición a la configuración de fábrica Si al restablecer la configuración de fábrica está conectado un C-PLUG, se borra el contenido del C-PLUG.

Uso de un C-PLUG no nuevo

Utilice sólo C-PLUGs formateados para el respectivo tipo de módulo SCALANCE S. C-PLUGs utilizados ya en equipos de otros tipos y formateados para los mismos no se deben emplear.

Vea en la tabla siguiente qué C-PLUG se puede utilizar para qué tipo de módulo SCALANCE S:

Tipo de módulo SCALANCE S	C-PLUG formateado por		
	S602	S612	S613
S602	X	-	-
S612	-	X	x *)
S613	-	X	X

- **X** C-PLUG utilizable con el tipo de módulo
- **-** C-PLUG no utilizable con el tipo de módulo
- ***)** La compatibilidad depende de los recursos.

Extracción del C-PLUG

Sólo es necesario extraer el C-PLUG en caso de fallo (avería de hardware) del equipo básico.

ATENCIÓN
Observe el estado operativo ¡Sólo se debe retirar el C-PLUG en estado sin tensión!

Diagnóstico

La conexión de un C-PLUG que contenga la configuración de un tipo de equipo no compatible, la desconexión no intencionada del C-PLUG o funciones incorrectas en general del C-PLUG son señalizadas por los mecanismos de diagnóstico del equipo terminal (indicador LED Fault).

2.5 Transferir firmware

Nuevas ediciones de firmware se pueden cargar con la herramienta de configuración Security Configuration Tool en los módulos SCALANCE S.

Requisitos

Para la transferencia de un nuevo firmware a un módulo SCALANCE S se tienen que cumplir los siguientes requisitos:

- Ha de tener derechos de administrador para el proyecto;
- SCALANCE S tiene que estar configurado con una dirección IP.

La transferencia es segura

La transferencia del firmware tiene lugar a través de una conexión segura, por lo que se puede realizar también desde la red no protegida.

El firmware en sí está signado y codificado. Con esto se garantiza que sólo se pueda cargar firmware auténtico en el módulo SCALANCE S.

La transferencia se puede realizar durante el funcionamiento normal

El firmware se puede transferir durante el funcionamiento normal de un módulo SCALANCE S. Sin embargo, la comunicación se interrumpe durante el tiempo posterior al proceso de carga, hasta el transcurso automático del rearranque de SCALANCE S. Un nuevo firmware cargado sólo está activo tras este rearranque del módulo SCALANCE S.

Si la trasferencia ha sufrido una perturbación y se ha cancelado, el módulo vuelve a arrancar con la versión de firmware antigua.

Procedimiento a seguir para la transferencia

Seleccione el siguiente comando de menú:

Transfer ▸ Firmware Update...

GETTING STARTED 3

Rápidamente a la meta con GETTING STARTED

Por medio de una red de test simple aprenderá aquí el manejo del SCALANCE S y de la herramienta de configuración Security Configuration Tool. Verá cómo se pueden implementar ya en la red las funciones de protección de SCALANCE S sin grandes trabajos de configuración.

Puede implementar al respecto en diferentes ejemplos de seguridad las funciones fundamentales de SCALANCE S / SOFTNET Security Client:

- Con SCALANCE S612 / S613:
  - Configuración de una VPN con SCALANCE S como puntos finales de un túnel IPsec
  - Configuración de una VPN con SCALANCE S y SOFTNET Security Client como puntos finales de un túnel IPsec
- Con todos los módulos SCALANCE S:
  - Configuración de SCALANCE S como Firewall
  - Configuración de SCALANCE S como Router NAT/NAPT y Firewall
- Con SOFTNET Security Client
  - Configuración de una VPN con SCALANCE S y SOFTNET Security Client como puntos finales de un túnel IPsec
  - Configuración de una VPN con MD741-1 y SOFTNET Security Client como puntos finales de un túnel IPsec

Si desea saber más

Encontrará más informaciones en los capítulos siguientes de este manual. En ellos se explican con detalle todas las funciones.

Nota

Los ajustes de IP utilizados en los ejemplos se han elegido libremente y funcionan sin conflictos en la red de test aislada.

Al trabajar con una red real se tienen que adaptar estos ajustes de IP al entorno de la red, a fin de evitar eventuales conflictos de direcciones.

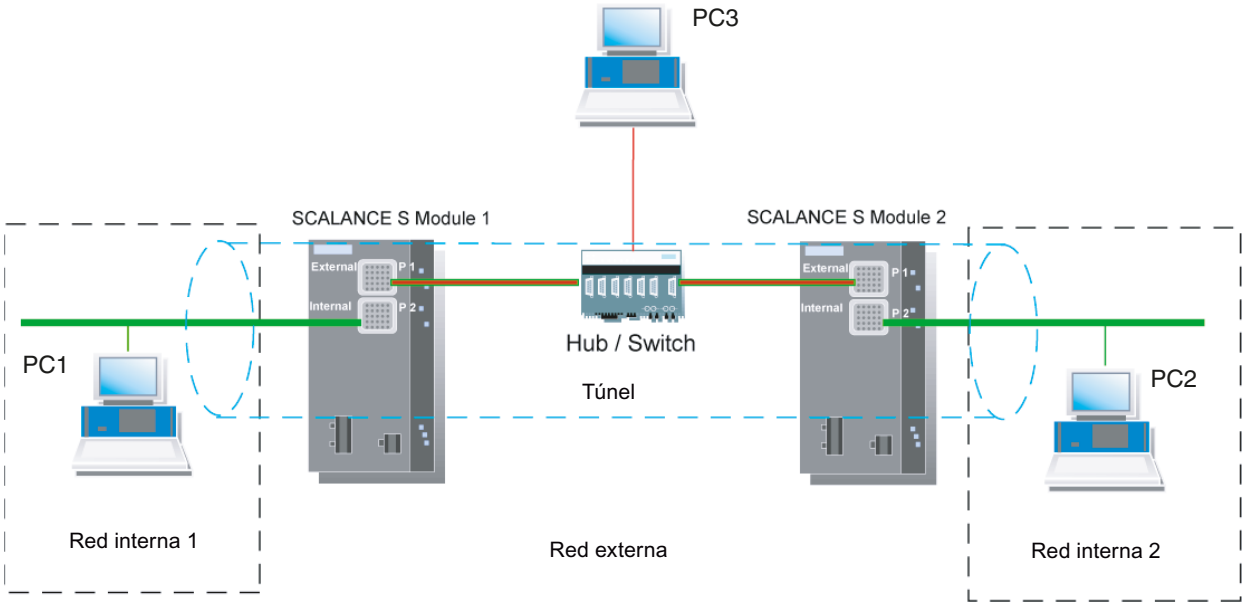
3.1 Ejemplo 1: Túnel VPN - Ejemplo de túnel IPsec con SCALANCE S612 / S613

3.1.1 Resumen

En este ejemplo se configura la función Túnel en la vista de configuración "Standard Mode". SCALANCE S Module 1 y SCALANCE S Module 2 constituyen en este ejemplo los dos puntos finales del túnel para la conexión de túnel protegida.

Con esta configuración se consigue que el tráfico IP y el tráfico de la Layer 2 (sólo en el modo bridge) sólo sea posible a través de las conexiones de túnel establecidas emtre interlocutores autorizados.

Construcción de la red de test



- Red interna - conexión a SCALANCE S Port 2 (puerto "Internal Network")

  En la estructura de test, en la red interna cada nodo de red se realiza por medio de un PC que está conectado al puerto "Internal Network" (Port 2, verde) de un módulo SCALANCE S.

  – PC1: Representa a una estación participante en la red interna 1

  – PC2: Representa a una estación participante en la red interna 2

  – SCALANCE S Module 1: Módulo SCALANCE S para la red interna 1

  – SCALANCE S Module 2: Módulo SCALANCE S para la red interna 2

- Red externa - conexión a SCALANCE S Port 1 (puerto "External Network")

  La red pública ("red externa") se conecta al puerto "External Network" (Port 1, rojo) de un módulo SCALANCE S.

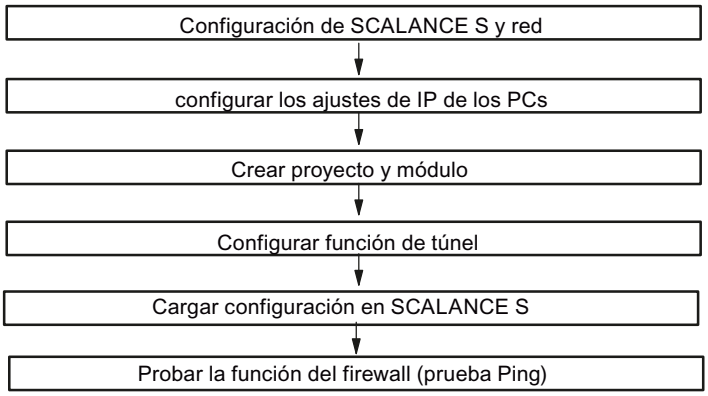
  PC3: PC con el software de configuración Security Configuration Tool

Dispositivos/componentes necesarios:

Utilice los siguientes componentes para el montaje:

- 2 módulos SCALANCE S (opcional: uno o dos rieles de perfil de sombrero correspondientemente instalados, con material de montaje);
- 1 ó 2 dispositivos de alimentación eléctrica de 24V con conectores de cables y enchufes de bloques de bornes (ambos módulos pueden funcionar también con un dispositivo de alimentación eléctrica común) ;
- 1 PC en el que esté instalada la herramienta de configuración "Security Configuration Tool";
- 2 PCs en las redes internas, para el test de la configuración;
- 1 hub o switch de red para el establecimiento de conexiones de red con los dos SCALANCE S así como los PCs/PGs;
- los necesarios cables de red, cables TP (Twisted Pair) según el estándar IE FC RJ45 para Industrial Ethernet.

Los pasos siguientes, en síntesis:


Configuración de SCALANCE S y red
configurar los ajustes de IP de los PCs
Crear proyecto y módulo
Configurar función de túnel
Cargar configuración en SCALANCE S
Probar la función del firewall (prueba Ping)

3.1.2 Poner a punto los SCALANCE S y la red

Procedimiento a seguir:

1. Saque primero los equipos SCALANCE S de su embalaje y compruebe si están en perfecto estado.
2. Conecte la alimentación de tensión a SCALANCE S.

Resultado: Tras conectar la tensión de servicio brilla el diodo Fault (F) con luz amarilla.

⚠ ADVERTENCIA

El equipo SCALANCE S está previsto para funcionar con baja tensión de seguridad. En consecuencia, a las conexiones de alimentación sólo se deben conectar bajas tensiones de seguridad (SELV) según IEC950/EN60950/ VDE0805.

La fuente de alimentación utilizada para el SCALANCE S tiene que ser del tipo NEC Class 2 (gama de tensión 18-32 V, consumo de corriente aprox. 250 mA).

Para el montaje y la conexión de los módulos SCALANCE S, tenga en cuenta el capítulo "Propiedades del producto y puesta en servicio".

1. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45):

– Conecte PC1 al Port 2 de Module 1 y PC2 al Port 2 de Module 2.
– Conecte Port 1 de Module 1 y Port 1 de Module 2 al Hub/Switch.
– Conecte también PC3 al Hub/Switch.

2. Encienda los PCs participantes.

ATENCIÓN
Las conexiones de Ethernet en Port 1 y Port 2 son tratadas de forma diferente por el SCALANCE S, por lo que no se deben confundir al establecer la conexión con la red de comunicación: • Port 1 - External Network conector hembra RJ45 superior, marca roja = área de red no protegida; • Port 2 - Internal Network conector hembra RJ45 inferior, marca verde = red protegida por SCALANCE S Si se permutan los puertos, el equipo pierde su función de protección.

3.1.3 Preparar los ajustes de IP de los PCs

Los PCs deberían tener los siguientes ajustes de dirección IP para el test:

PC	Dirección IP	Máscara de subred
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0
PC3	191.0.0.3	255.255.0.0

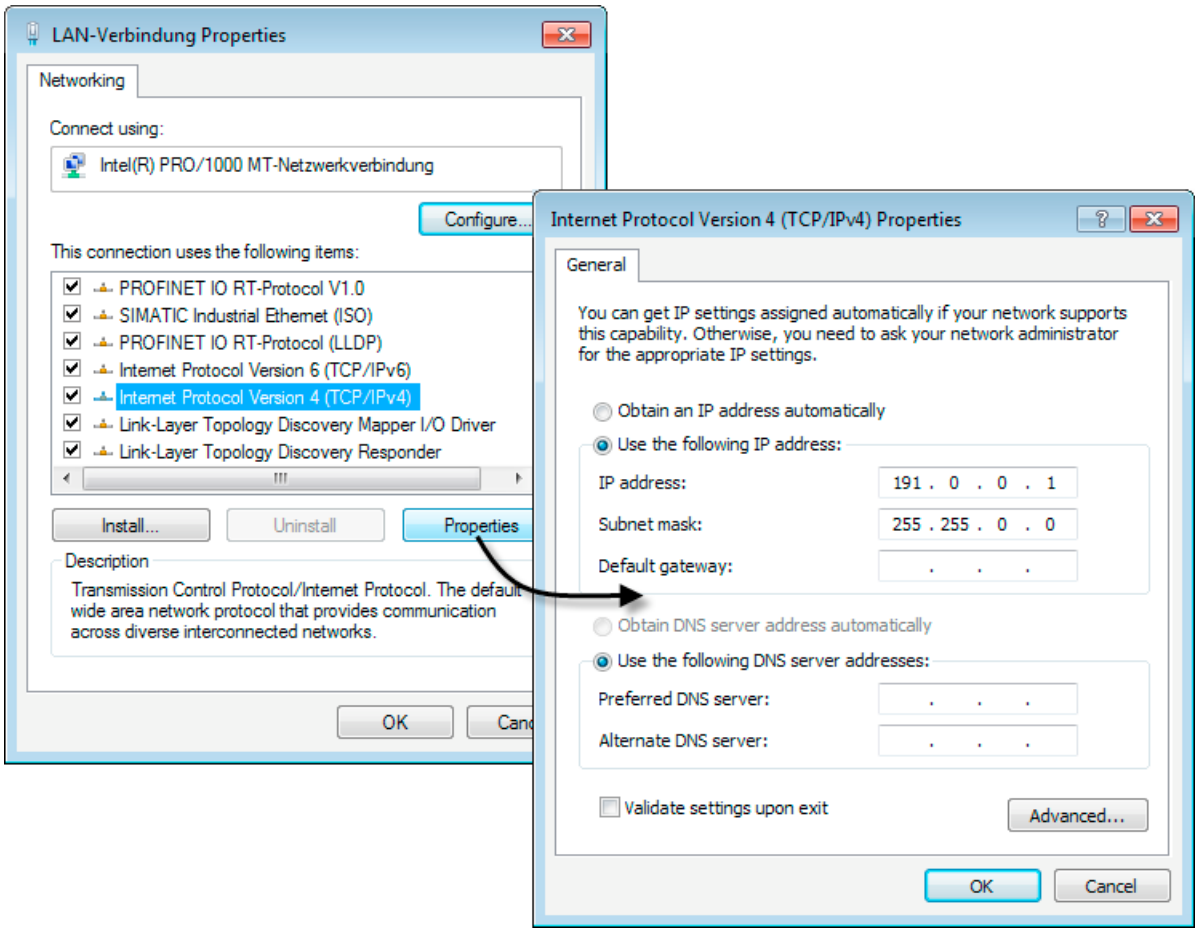
Proceda del siguiente modo para PC1, PC2 y PC3:

1. Abra el panel de control en el respectivo PC con el siguiente comando de menú:

   Inicio ▸ Panel de control

2. Abra el símbolo "Red y centro de autorización" y, en el menú de navegación que se encuentra a la izquierda, seleccione la opción "Modificar los ajustes del adaptador".

3. Active en el diálogo "Propiedades de la conexión LAN" la casilla de opción "Protocolo Internet versión 4 (TCP/IPv4)" y haga clic en el botón "Propiedades".


LAN-Verbindung Properties
Networking
Connect using:
Intel(R) PRO/1000 MT-Netzwerkverbindung
Configure...
This connection uses the following items:
PROFINET IO RT-Protocol V1.0
SIMATIC Industrial Ethernet (ISO)
PROFINET IO RT-Protocol (LLDP)
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
191 . 0 . 0 . 1
Subnet mask:
255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4. Seleccione en el diálogo "Propiedades del protocolo de Internet versión 4 (TCP/IPv4)" la casilla de verificación "Usar la siguiente dirección IP:" e introduzca en los campos previstos al efecto los valores correspondientes al PC, tomados de la tabla "*Crear configuración IP de los PCs*".

   Cierre los cuadros de diálogo con "Aceptar" y salga del panel de control.

3.1.4 Crear proyecto y módulos

Proceda del siguiente modo:

1. Inicie el software de configuración Security Configuration Tool en PC3.
2. Cree un nuevo proyecto con el siguiente comando de menú:

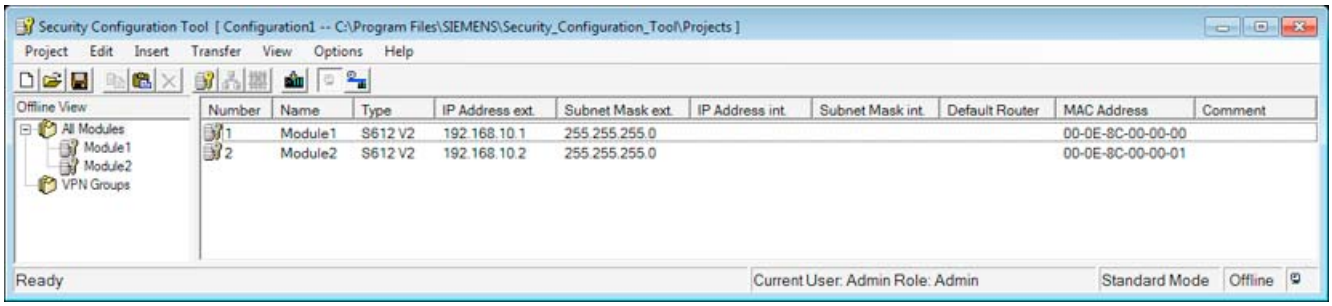
   Project ▸ New

   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted entra aquí se le asigna el papel de un administrador.

3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto crea un nuevo proyecto.
4. Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software". Configure ahora el tipo de producto, el módulo y la versión de firmware, cerrando al final el diálogo pulsando "OK".
5. Cree un segundo módulo con el siguiente comando de menú:
   Insert ▸ Module

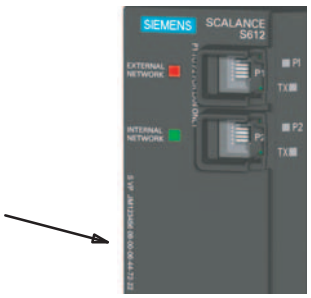
   Configure ahora el tipo de producto, el módulo y la versión de firmware, cerrando al final el diálogo pulsando "OK".

   A este módulo se le asigna automáticamente un nombre según lo ajustado previamente para el proyecto y los valores de parámetros también preajustados. La dirección IP se ha seguido contando respecto a la de "Module 1", siendo pues diferente.

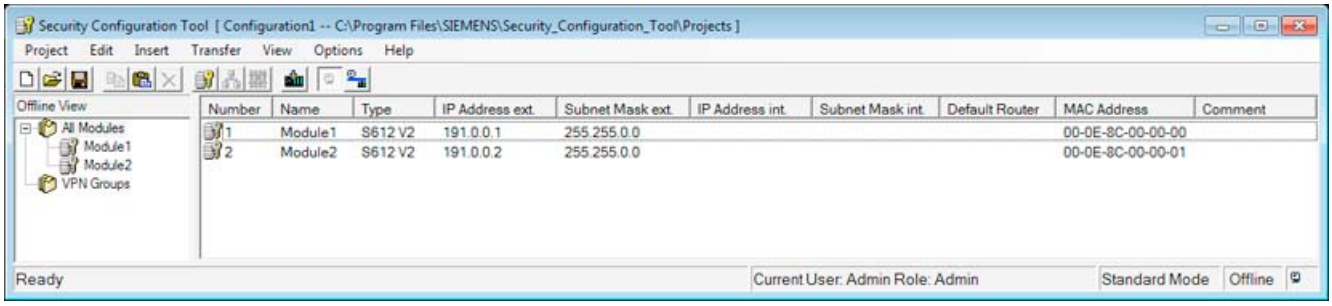

Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects]
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 00-0E-8C-00-00-00
2 Module2 S612 V2 192.168.10.2 255.255.255.0 00-0E-8C-00-00-01
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

6. Haga clic en el área de navegación en "All Modules" y a continuación en el área de contenido, en la línea con "Module 1".
7. Haga clic ahora en la columna "MAC Address" e introduzca ésta en el formato predeterminado.

   Encontrará esta dirección en la cara frontal del módulo SCALANCE S (vea la figura)



8. Haga clic ahora en la columna "IP Address ext." e introduzca ésta en el formato predeterminado; adapte también la máscara de subred.
   - para el módulo 1: Dirección IP: 191.0.0.201 Máscara de subred: 255.255.0.0
   - para el módulo 2: Dirección IP: 191.0.0.202 Máscara de subred: 255.255.0.0


Security Configuration Tool [Configuration1 -- C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects]
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 191.0.0.1 255.255.0.0 00-0E-8C-00-00-00
2 Module2 S612 V2 191.0.0.2 255.255.0.0 00-0E-8C-00-00-01
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

9. Repita los pasos 6 hasta 8 con "Module 2".

3.1.5 Configurar conexión túnel

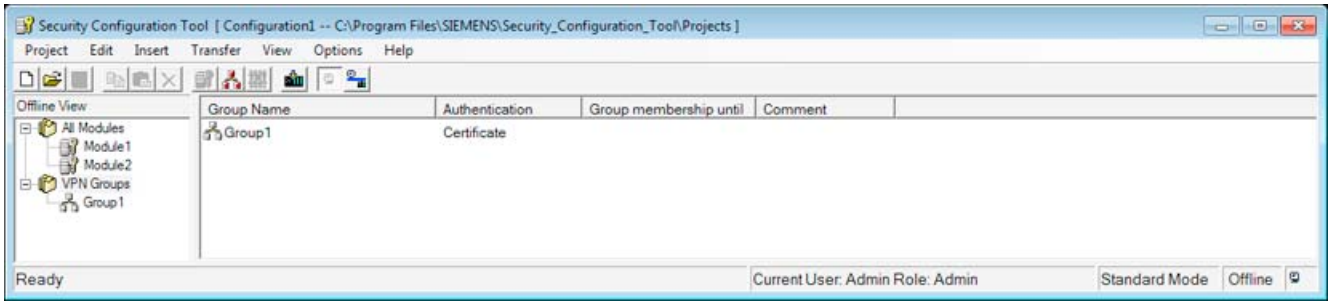
Dos SCALANCE S pueden crear exactamente un túnel IPSec para la comunicación segura si están asignados a un mismo grupo en el proyecto.

Proceda del siguiente modo:

1. Seleccione en el área de navegación "All Groups" y cree un nuevo grupo con el siguiente comando de menú:

   Insert ▸ Group

   Este grupo recibe automáticamente el nombre "Group 1".



2. Seleccione en el área de contenido el módulo de SCALANCE S "Module 1" y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora a ese grupo o bien es miembro de ese grupo.

   El color del símbolo de llave del icono de módulo cambia ahora de gris a azul.

3. Seleccione en el área de contenido el módulo de SCALANCE S "Module 2" y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora también a ese grupo.

4. Guarde ahora este proyecto con el siguiente comando de menú, bajo un nombre apropiado:

   Project ▸ Save As…

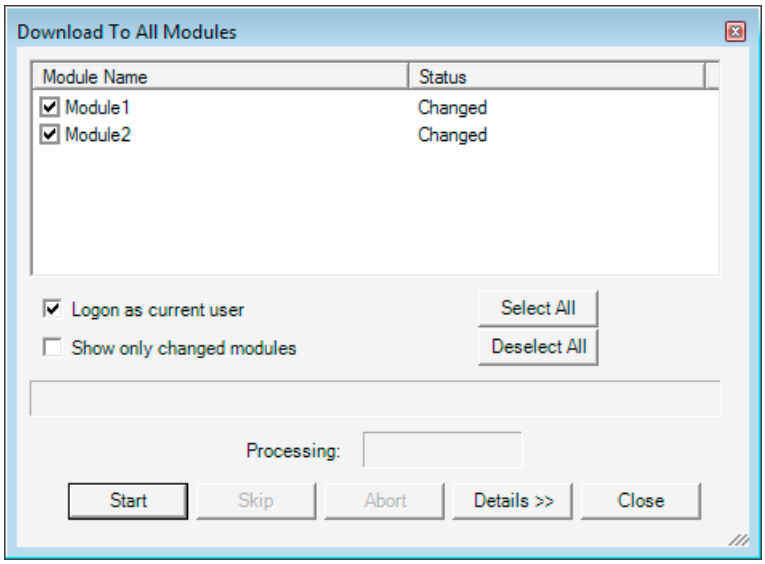
Con esto ha terminado la configuración de la conexión de túnel.

3.1.6 Cargar la configuración en SCALANCES S

Proceda del siguiente modo:

1. Llame el siguiente cuadro de diálogo con el comando aquí indicado:

   Transfer ▸ To All Modules…



2. Seleccione ambos módulos por medio del botón "Select All".
3. Inicie el proceso de carga con el botón "Start".

Si el proceso de carga se ha concluido sin errores, el SCALANCE S arranca de nuevo automáticamente y se activa la nueva configuración.

Resultado: SCALANCE S en modo productivo

SCALANCE S se encuentra ahora en el modo productivo. Este estado es señalizado por el diodo indicador Fault con luz verde.

Con esto ha concluido la puesta en servicio de la configuración y los dos SCALANCE S pueden crear un túnel de comunicación a través del que se pueden comunicar de forma segura los nodos de las dos redes internas.

3.1.7 Probar la función túnel (Ping-Test)

¿Cómo se puede probar la función configurada?

La prueba de la función se puede realizar con un comando "ping" tal como se describe a continuación.

Como alternativa se pueden utilizar otros programas de comunicación para el test de la configuración.

ATENCIÓN
En caso de Windows, el cortafuegos (firewall) puede estar ajustado como estándar de manera que no puedan pasar comandos PING. Eventualmente tendrá que habilitar los servicios ICMP del tipo Request y Response.

Sección de test 1

Compruebe ahora el funcionamiento de la conexión de túnel establecida entre PC1 y PC2 del siguiente modo:

1. En el PC2, llame en la barra de inicio el siguiente comando de menú:

   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

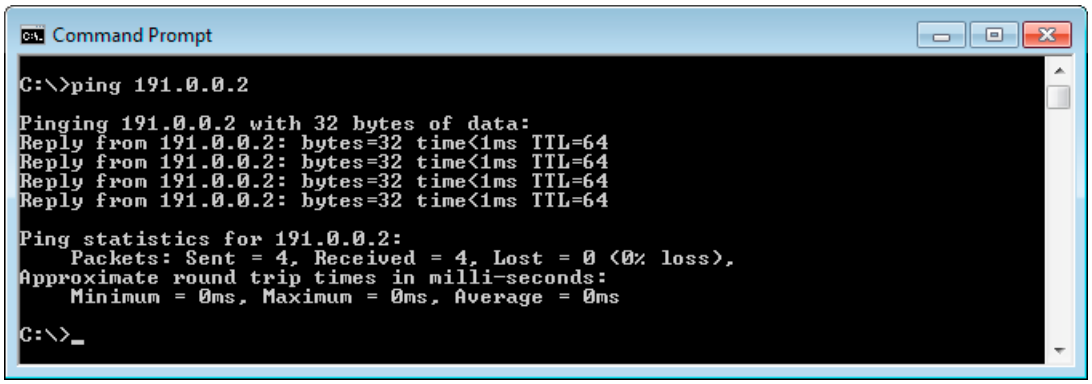
2. Entrada del comando ping de PC1 a PC2 (dirección IP 191.0.0.2)

   Directamente en la línea de comandos de la ventana presentada "Símbolo del sistema", introduzca en la posición del cursor el comando

   ping 191.0.0.2.

   conectado.

   Aparecerá entonces el siguiente mensaje: (respuesta positiva del PC2).



Resultado

Cuando los telegramas IP llegan al PC2, la "estadística Ping" muestra para 191.0.0.2 lo siguiente:

- Enviado = 4
- Recibido = 4
- Perdido = 0 (0% pérdida)

Dado que no estaba permitida ninguna otra comunicación, esto telegramas sólo se pueden haber transportado por el túnel VPN.

Sección de test 2

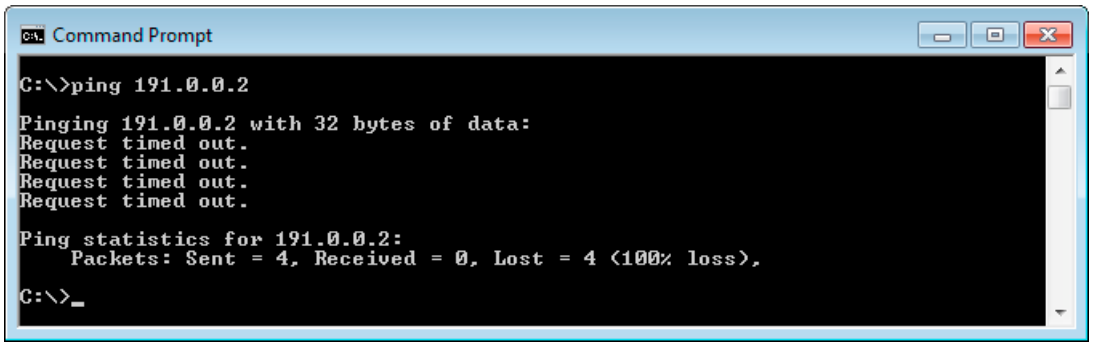
Repita ahora el test emitiendo un comando ping desde el PC3.

1. En el PC3, llame en la barra de inicio el siguiente comando de menú:

   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

2. Emita de nuevo el mismo comando ping (**ping 191.0.0.2**) en la ventana del símbolo del sistema de PC3.

   Aparecerá entonces el siguiente mensaje: (no hay respuesta del PC2).


Command Prompt
C:\>ping 191.0.0.2
Pinging 191.0.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 191.0.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

Resultado

Los telegramas IP del PC3 no pueden llegar al PC2, ya que no hay configurada ninguna comunicación túnel entre estos equipos ni tampoco se permite el tráfico de datos IP normal.

Esto se indica en la "estadística Ping" para 191.0.0.2 del siguiente modo:

- Enviado = 4
- Recibido = 0
- Perdido = 4 (100% pérdida)

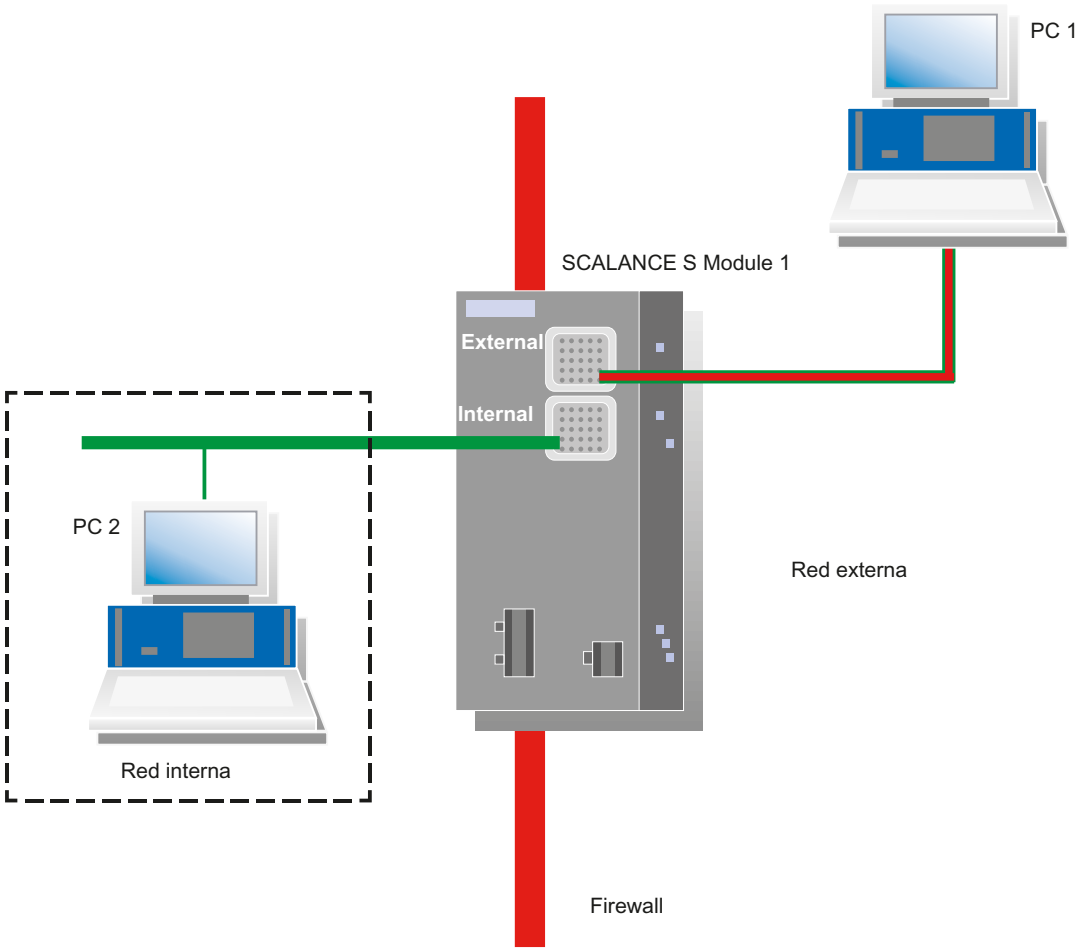
3.2 Ejemplo 2: Firewall - Uso del SCALANCE S como Firewall

3.2.1 Resumen

En este ejemplo se configura el firewall en la vista de configuración "Standard Mode". El modo estándar contiene bloques de reglas definidos para el tráfico de datos.

Con esta configuración se consigue que el tráfico IP sólo pueda ser iniciado por la red interna; desde la red externa sólo se permite la respuesta.

Construcción de la red de test



- Red interna - conexión a SCALANCE S Port 2

  En la estructura de test, en la red interna cada nodo de red se realiza por medio de un PC que está conectado al puerto "Internal Network" (Port 2, verde) de un módulo SCALANCE S.

  – PC2: Representa a una estación participante en la red interna

  – SCALANCE S Module 1: Módulo SCALANCE S para la red interna

- Red externa - conexión a SCALANCE S Port 1

  La red pública ("red externa") se conecta al puerto "External Network" (Port 1, rojo) de un módulo SCALANCE S.

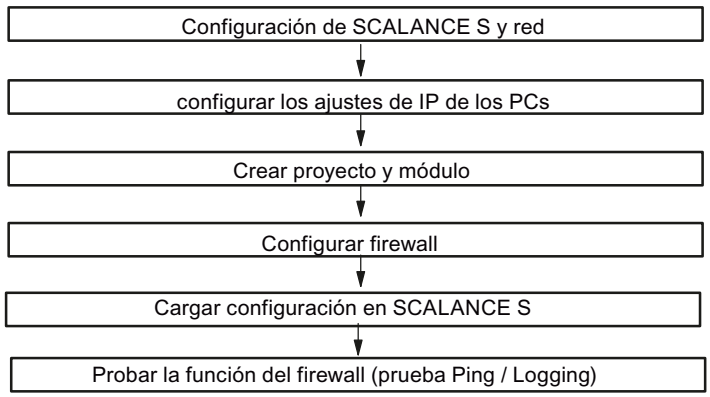
  – PC1: PC con el software de configuración Security Configuration Tool

Dispositivos/componentes necesarios:

Utilice los siguientes componentes para el montaje:

- 1 SCALANCE S, (adicionalmente, como opción: un riel de perfil de sombrero correspondientemente instalado, con material de montaje)
- 1 alimentación eléctrica de 24V con conexiones de cables y conectores de bloque de bornes
- 1 PC en el que esté instalada la herramienta de configuración "Security Configuration Tool"
- 1 PC en la red interna, para test de la configuración
- los necesarios cables de red, cables TP (Twisted Pair) según el estándar IE FC RJ45 para Industrial Ethernet.

Los pasos siguientes, en síntesis:


Configuración de SCALANCE S y red
configurar los ajustes de IP de los PCs
Crear proyecto y módulo
Configurar firewall
Cargar configuración en SCALANCE S
Probar la función del firewall (prueba Ping / Logging)

3.2.2 Poner a punto los SCALANCE S y la red

Proceda del siguiente modo:

1. Saque primero el SCALANCE S de su embalaje y compruebe si está en perfecto estado.
2. Conecte la alimentación de tensión a SCALANCE S.

   Resultado: Tras conectar la tensión de servicio brilla el diodo Fault (F) con luz amarilla.

⚠ ADVERTENCIA

El equipo SCALANCE S está previsto para funcionar con baja tensión de seguridad. En consecuencia, a las conexiones de alimentación sólo se deben conectar bajas tensiones de seguridad (SELV) según IEC950/EN60950/ VDE0805.

La fuente de alimentación utilizada para el SCALANCE S tiene que ser del tipo NEC Class 2 (gama de tensión 18-32 V, consumo de corriente aprox. 250 mA).

Para el montaje y la conexión de los módulos SCALANCE S, tenga en cuenta el capítulo "Propiedades del producto y puesta en servicio".

3. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45):
   - Conecte el PC2 al puerto 2 del Module 1.
   - Conecte el PC1 al puerto 1 del Module 1.
4. Encienda los PCs participantes.

ATENCIÓN

Las conexiones de Ethernet en Port 1 y Port 2 son tratadas de forma diferente por el SCALANCE S, por lo que no se deben confundir al establecer la conexión con la red de comunicación:

- Port 1 - External Network
  conector hembra RJ45 superior, marca roja = área de red no protegida;
- Port 2 - Internal Network
  conector hembra RJ45 inferior, marca verde = red protegida por SCALANCE S;

Si se permutan los puertos, el equipo pierde su función de protección.

3.2.3 Preparar los ajustes de IP de los PCs

Los PCs deberían tener los siguientes ajustes de dirección IP para el test:

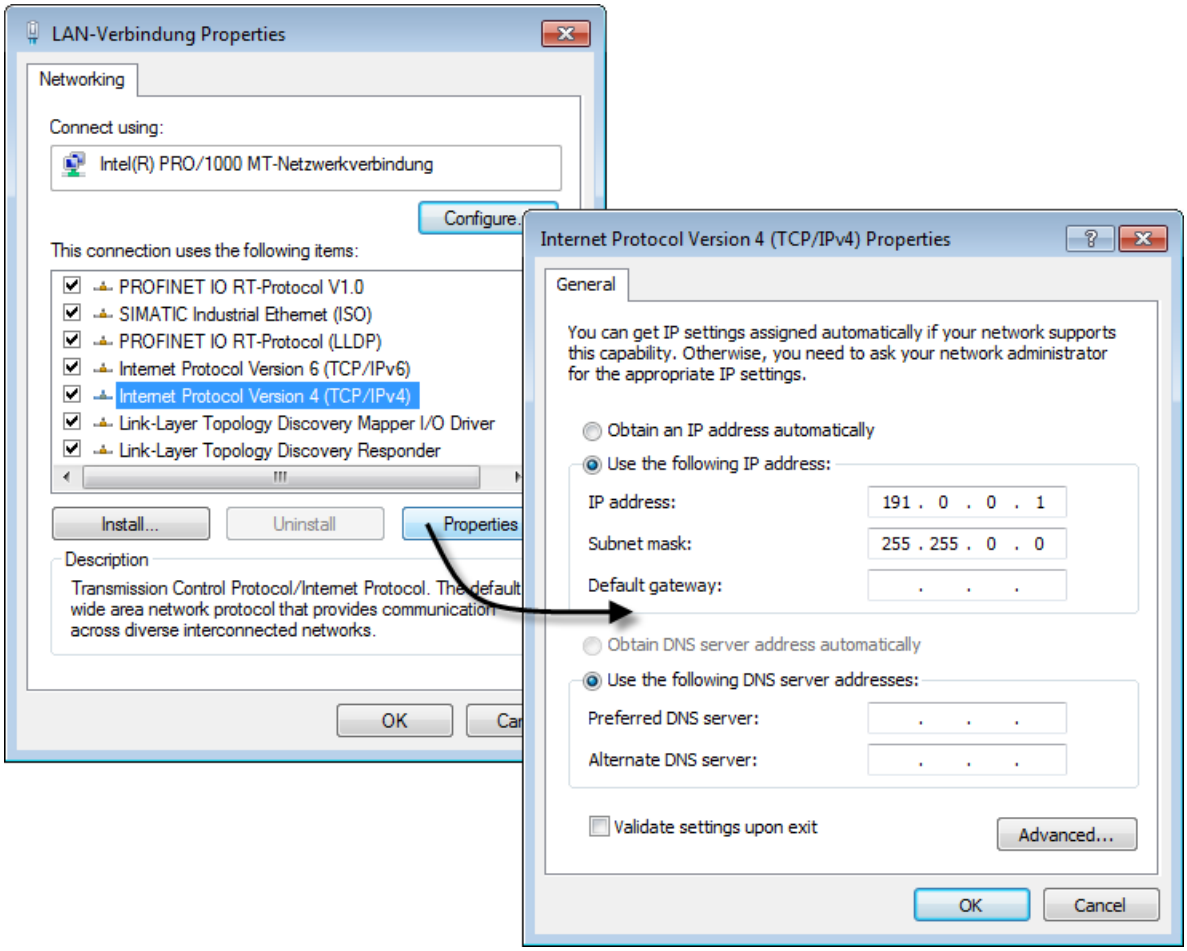
PC	Dirección IP	Máscara de subred
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0

Para ello, proceda del siguiente modo en el PC1 y el PC2:

1. Abra el panel de control en el respectivo PC con el siguiente comando de menú:

   Inicio ▸ Panel de control

2. Abra el símbolo "Red y centro de autorización" y, en el menú de navegación que se encuentra a la izquierda, seleccione la opción "Modificar los ajustes del adaptador".
3. Active en el diálogo "Propiedades de la conexión LAN" la casilla de opción "Protocolo Internet versión 4 (TCP/IPv4)" y haga clic en el botón "Propiedades".


LAN-Verbindung Properties
Networking
Connect using:
Intel(R) PRO/1000 MT-Netzwerkverbindung
Configure...
This connection uses the following items:
PROFINET IO RT-Protocol V1.0
SIMATIC Industrial Ethernet (ISO)
PROFINET IO RT-Protocol (LLDP)
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default
wide area network protocol that provides communication
across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
191 . 0 . 0 . 1
Subnet mask:
255 . 255 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4. Seleccione en el diálogo "Propiedades del protocolo de Internet versión 4 (TCP/IPv4)" la casilla de verificación "Usar la siguiente dirección IP:" e introduzca en los campos previstos al efecto los valores correspondientes al PC, tomados de la tabla "*Crear configuración IP de los PCs*".

   Cierre los cuadros de diálogo con "Aceptar" y salga del panel de control.

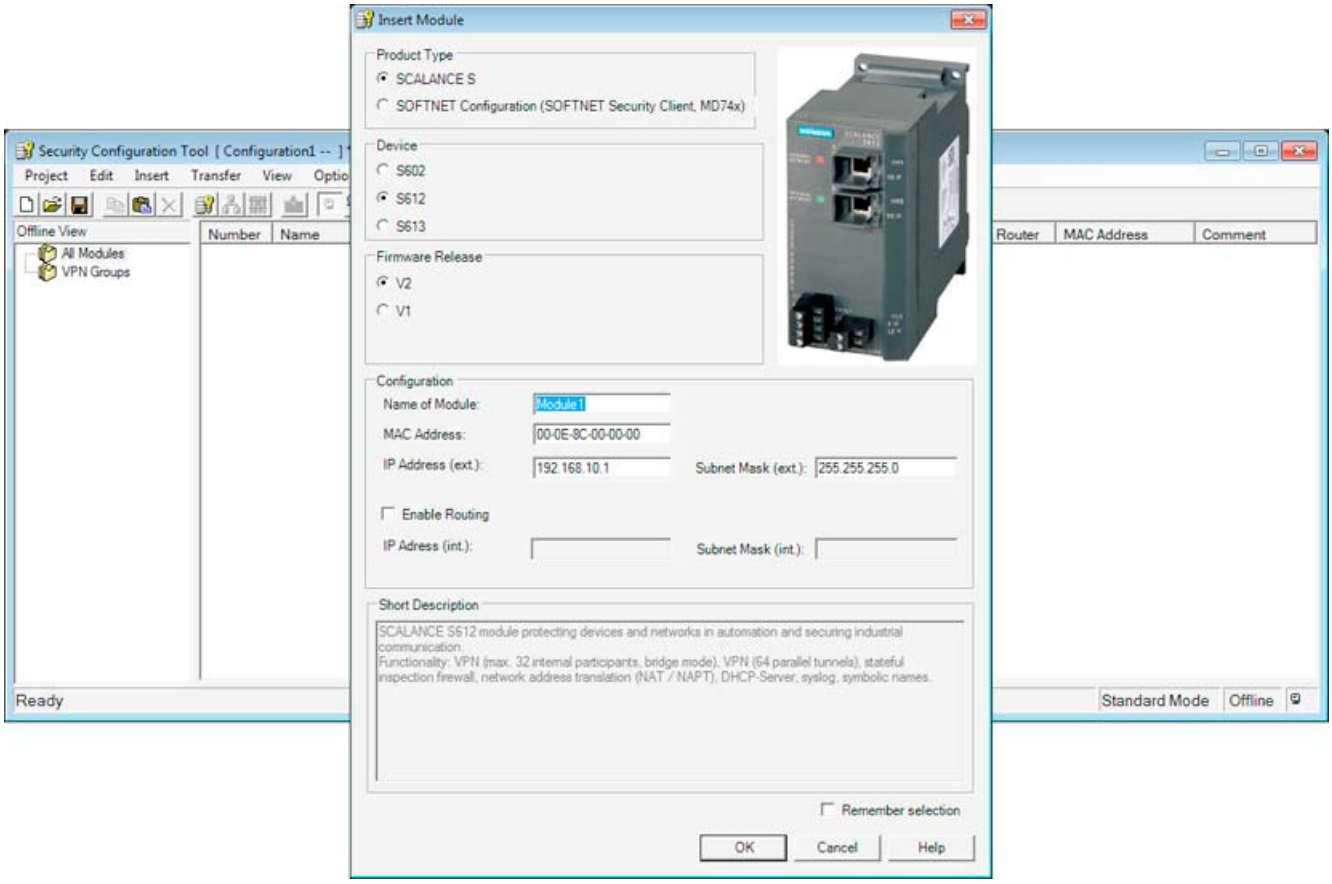
3.2.4 Crear proyecto y módulo

Proceda del siguiente modo:

1. Instala e inicie el software de configuración "Security Configuration Tool" en el PC1.
2. Cree un nuevo proyecto con el siguiente comando de menú:

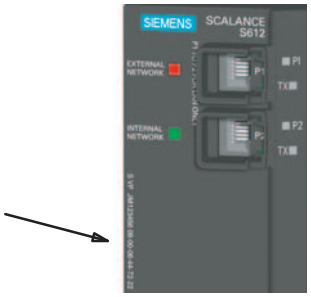
   Project ▸ New

   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted entra aquí se le asigna el papel de un administrador.
3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto crea un nuevo proyecto.

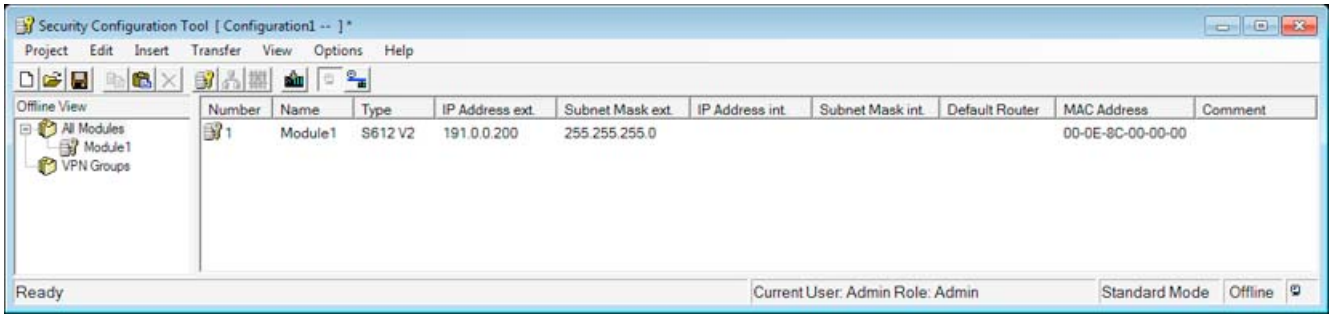


4. Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software". Configure ahora su tipo de producto, el módulo y la versión de firmware.

5. Introduzca en el campo de la "Dirección MAC" en el área de "Configuración" la dirección MAC impresa en la carcasa del módulo en el formato especificado.
   Podrá encontrar esta dirección en la página principal del módulo SCALANCE S (véase la figura).



6. Introduzca también en el formato preestablecido la dirección IP externa (191.0.0.200) y la máscara de subred externa (255.255.0.0), y confirme el diálogo con "OK". De ahí en adelante se incluirá su módulo en la lista de los módulos configurados.


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 191.0.0.200 255.255.255.0 00-0E-8C-00-00-00
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

3.2.5 Configurar firewall

En el Standard Mode se peuden manejar fácilmente los ajustes del Firewall gracias a bloques de reglas predefinidos. Haciendo clic se pueden activar estos bloques de reglas.

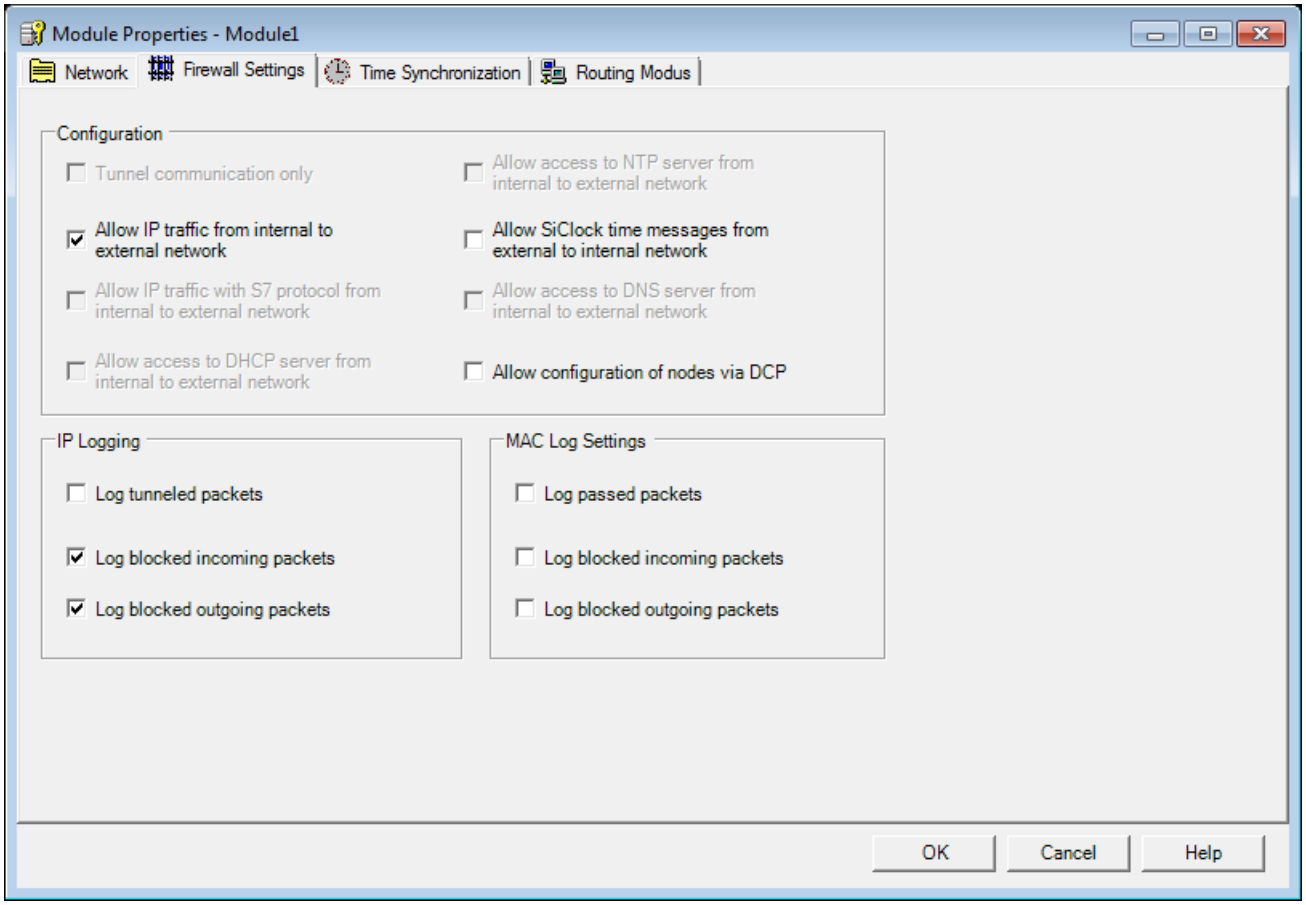
Proceda del siguiente modo:

1. Marque en el área de contenido la línea "Module 1".
2. Seleccione el siguiente comando de menú:

   Edit ▸ Properties…

3. En el cuadro de diálogo visualizado, seleccione la ficha "Firewall".

4. Active la opción en la forma aquí representada:


Module Properties - Module1
Network
Firewall Settings
Time Synchronization
Routing Modus
Configuration
Tunnel communication only
Allow access to NTP server from internal to external network
Allow IP traffic from internal to external network
Allow SiClock time messages from external to internal network
Allow IP traffic with S7 protocol from internal to external network
Allow access to DNS server from internal to external network
Allow access to DHCP server from internal to external network
Allow configuration of nodes via DCP
IP Logging
Log tunneled packets
Log blocked incoming packets
Log blocked outgoing packets
MAC Log Settings
Log passed packets
Log blocked incoming packets
Log blocked outgoing packets
OK
Cancel
Help

   Con esto se consigue que el tráfico IP sólo pueda ser iniciado por la red interna; desde la red externa sólo se permite la respuesta.

5. Seleccione adicionalmente las opciones Log para registrar el tráfico de datos.
6. Cierre el cuadro de diálogo con "OK".
7. Guarde ahora este proyecto con el siguiente comando de menú, bajo un nombre apropiado:

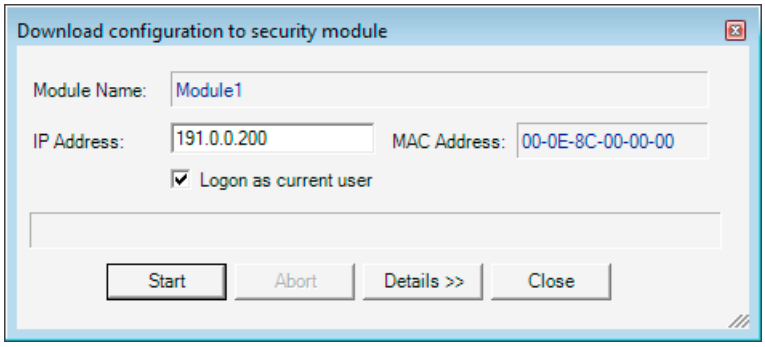
   Project ▸ Save As…

3.2.6 Cargar la configuración en SCALANCES S

Proceda del siguiente modo:

1. Seleccione el módulo en el área de contenido.
2. Seleccione el siguiente comando de menú:

   Transfer ▸ To Module...



3. Inicie el proceso de carga con el botón "Start".

Si el proceso de carga se ha concluido sin errores, el SCALANCE S arranca de nuevo automáticamente y se activa la nueva configuración.

Resultado: SCALANCE S en modo productivo

SCALANCE S se encuentra ahora en el modo productivo. Este estado es señalizado por el diodo indicador Fault con luz verde.

Con esto ha terminado la puesta en servicio de la configuración y el SCALANCE S protege ahora, con el firewall instalado, la red interna (PC 2) conforme a la regla configurada: "Permitir tráfico IP de red interna a externa".

3.2.7 Probar la función Firewall (Ping-Test)

¿Cómo se puede probar la función configurada?

La prueba de la función se puede realizar con un comando "ping" tal como se describe a continuación.

Como alternativa se pueden utilizar otros programas de comunicación para el test de la configuración.

ATENCIÓN
En caso de Windows, el cortafuegos (firewall) puede estar ajustado como estándar de manera que no puedan pasar comandos PING. Eventualmente tendrá que habilitar los servicios ICMP del tipo Request y Response.

Sección de test 1

Pruebe ahora el funcionamiento de la configuración de firewall, primero con el tráfico de datos IP saliente permitido:

1. En el PC2, llame en la barra de inicio el siguiente comando de menú:

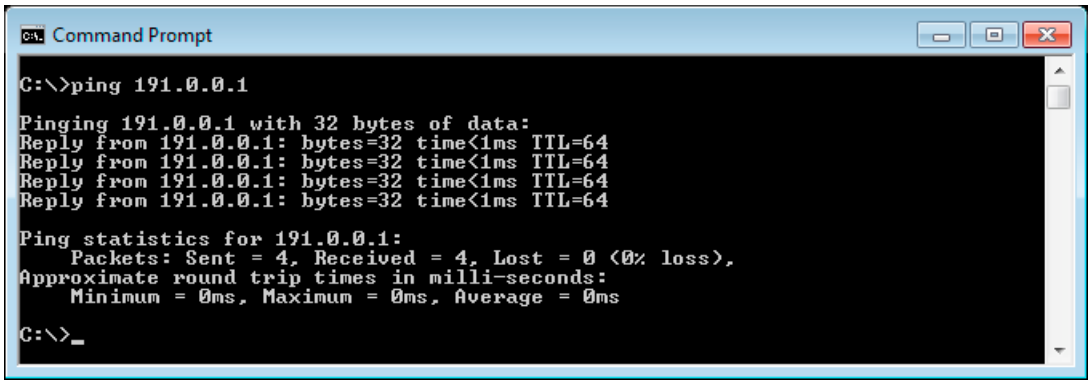
   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

2. Entrada del comando ping de PC2 a PC1 (dirección IP 191.0.0.1)

   Directamente en la línea de comandos de la ventana presentada "Símbolo del sistema", introduzca en la posición del cursor el siguiente comando:

   ping 191.0.0.1

   Aparecerá entonces el siguiente mensaje: (respuesta positiva del PC1).



Resultado

Cuando los telegramas IP llegan al PC1, la "estadística Ping" muestra para 191.0.0.1 lo siguiente:

- Enviado = 4
- Recibido = 4
- Perdido = 0 (0% pérdida)

Debido a la configuración, los telegramas ping han podido pasar de la red interna a la externa. El PC de la red externa ha respondido a los telegramas ping. Por la función "Stateful-Inspection" del firewall, los telegramas de respuesta que llegan ahora de la red externa son transmitidos automáticamente a la red interna.

Sección de test 2

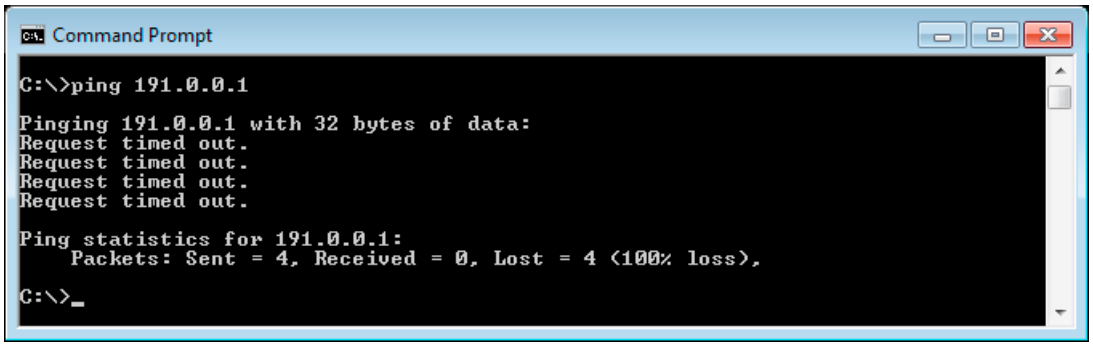
Pruebe ahora el funcionamiento de la configuración de firewall con el tráfico de datos IP saliente bloqueado:

1. Llame de nuevo el diálogo Firewall, tal como lo ha hecho antes.
2. Desactive ahora en la ficha "Firewall" la opción "Allow outgoing IP traffic" de la red interna a la red externa.

   Cierre el cuadro de diálogo con "OK".

3. Cargue ahora de nuevo la configuración modificada en el módulo SCALANCE S.
4. Una vez realizada la carga sin errores, introduzca de nuevo el mismo comando ping (**ping 191.0.0.1**) en la ventana del símbolo del sistema del PC2, tal como ya ha hecho antes.

   Aparecerá entonces el siguiente mensaje: (ninguna respuesta del PC1).


Command Prompt
C:\>ping 191.0.0.1
Pinging 191.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 191.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

Resultado

Los telegramas IP del PC2 no pueden llegar ahora al PC1, ya que no está permitido el tráfico de datos desde la "red interna" (PC2) a la "red externa" (PC1).

Esto se indica en la "estadística Ping" para 191.0.0.1 del siguiente modo:

- Enviado = 4
- Recibido = 0
- Perdido = 4 (100% pérdida)

3.2.8 Registro del tráfico de datos del firewall (Logging)

Como estándar, en el SCALANCE S está activado el registro local de eventos del sistema, de Audit y del filtro de paquetes.

Además, en el transcurso de este ejemplo ha activado, en la configuración del firewall, las opciones Log para todo el tráfico de datos.

Por consiguiente puede hacerse mostrar en el modo online los eventos registrados.

Proceda del siguiente modo:

1. Cambie ahora en el PC1 al modo online en la Security Configuration Tool con el siguiente comando de menú:

   View ▸ Online
2. Seleccione el siguiente comando de menú:

   Edit ▸ Online Diagnostics…
3. Seleccione la ficha "Packet Filter Log".

4. Accione el botón "Start Reading"
5. Confirme el cuadro de diálogo presentado con "OK".

   Resultado: Las entradas Log se leen del SCALANCE S y se presentan aquí.

3.3 Ejemplo 3: Firewall y Router - Uso del SCALANCE S como Firewall y Router

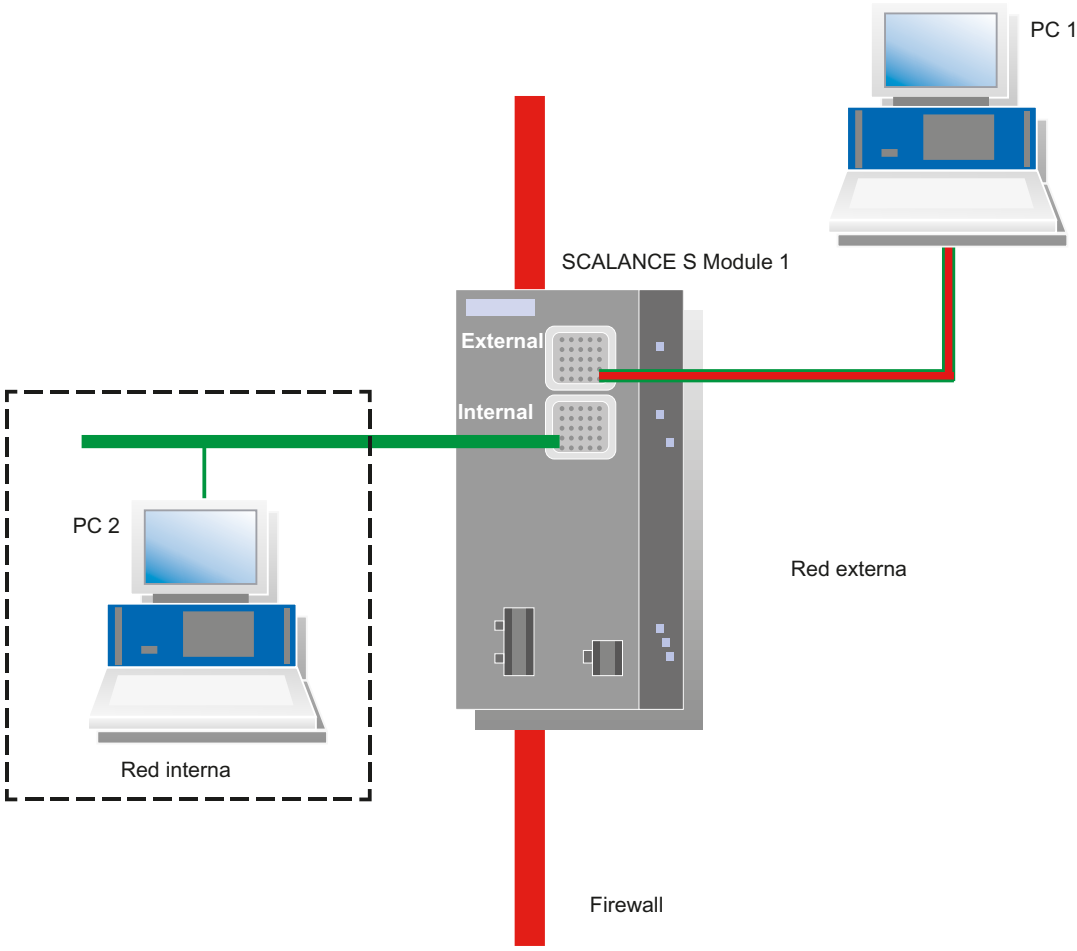
3.3.1 Resumen

En este ejemplo se configura el modo de Router NAT. La configuración se realiza en la vista de configuración "Advanced Mode".

Con la configuración aquí presentada consigue que puedan pasar el firewall (cortafuegos) todos los telegramas enviados desde la subred interna a estaciones PC1 participantes en la red externa. Los telegramas se transmiten al exterior con una dirección IP transformada a la dirección IP del SCALANCE S así como con un número de puerto asignado dinámicamente.

Desde la red externa sólo se permite la respuesta a estos telegramas.

Construcción de la red de test



- Red interna - conexión a SCALANCE S Port 2

  En la estructura de test, en la red interna cada nodo de red se realiza por medio de un PC que está conectado al puerto "Internal Network" (Port 2, verde) de un módulo SCALANCE S.

  – PC2: Representa a una estación participante en la red interna

  – SCALANCE S Module 1: Módulo SCALANCE S para la red interna

- Red externa - conexión a SCALANCE S Port 1

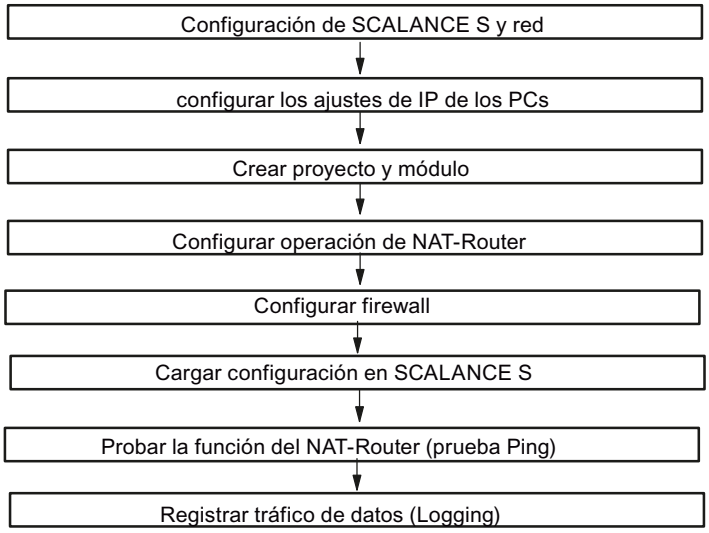
  La red pública ("red externa") se conecta al puerto "External Network" (Port 1, rojo) de un módulo SCALANCE S.
  PC1: PC con el software de configuración Security Configuration Tool

Dispositivos/componentes necesarios:

Utilice los siguientes componentes para el montaje:

- 1 SCALANCE S, (adicionalmente, como opción: un riel de perfil de sombrero correspondientemente instalado, con material de montaje);
- 1 alimentación eléctrica de 24V con conexiones de cables y conectores de bloque de bornes;
- 1 PC en el que esté instalada la herramienta de configuración "Security Configuration Tool";
- 1 PC en la red interna, para test de la configuración;
- los necesarios cables de red, cables TP (Twisted Pair) según el estándar IE FC RJ45 para Industrial Ethernet.

Los pasos siguientes, en síntesis:


Configuración de SCALANCE S y red
configurar los ajustes de IP de los PCs
Crear proyecto y módulo
Configurar operación de NAT-Router
Configurar firewall
Cargar configuración en SCALANCE S
Probar la función del NAT-Router (prueba Ping)
Registrar tráfico de datos (Logging)

3.3.2 Poner a punto los SCALANCE S y la red

Proceda del siguiente modo:

1. Saque primero el SCALANCE S de su embalaje y compruebe si está en perfecto estado.
2. Conecte la alimentación de tensión a SCALANCE S.

   Resultado: Tras conectar la tensión de servicio brilla el diodo Fault (F) con luz amarilla.

⚠ADVERTENCIA

El equipo SCALANCE S está previsto para funcionar con baja tensión de seguridad. En consecuencia, a las conexiones de alimentación sólo se deben conectar bajas tensiones de seguridad (SELV) según IEC950/EN60950/ VDE0805.

La fuente de alimentación utilizada para el SCALANCE S tiene que ser del tipo NEC Class 2 (gama de tensión 18-32 V, consumo de corriente aprox. 250 mA).

Para el montaje y la conexión de los módulos SCALANCE S, tenga en cuenta el capítulo 2 "Propiedades del producto y puesta en servicio".

3. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45):
   – Conecte el PC2 al puerto 2 del Module 1.
   – Conecte el PC1 al puerto 1 del Module 1.
4. Encienda los PCs participantes.

ATENCIÓN

Las conexiones de Ethernet en Port 1 y Port 2 son tratadas de forma diferente por el SCALANCE S, por lo que no se deben confundir al establecer la conexión con la red de comunicación:

- Port 1 - External Network, conector hembra RJ–45
  superior, marca roja = área de red no protegida;
- Port 2 - Internal Network
  conector hembra RJ45 inferior, marca verde = red protegida por SCALANCE S;

Si se permutan los puertos, el equipo pierde su función de protección.

3.3.3 Preparar los ajustes de IP de los PCs

Los PCs deberían tener los siguientes ajustes de dirección IP para el test:

PC	Dirección IP	Máscara de subred	Gateway estándar
PC1	192.168.10.100	255.255.255.0	192.168.10.1
PC2	172.10.10.100	255.255.255.0	172.10.10.1

Como Gateway estándar se han de indicar las direcciones IP que se asignan al módulo SCALANCE S en la configuración subsiguiente para la interfaz interna y la externa:

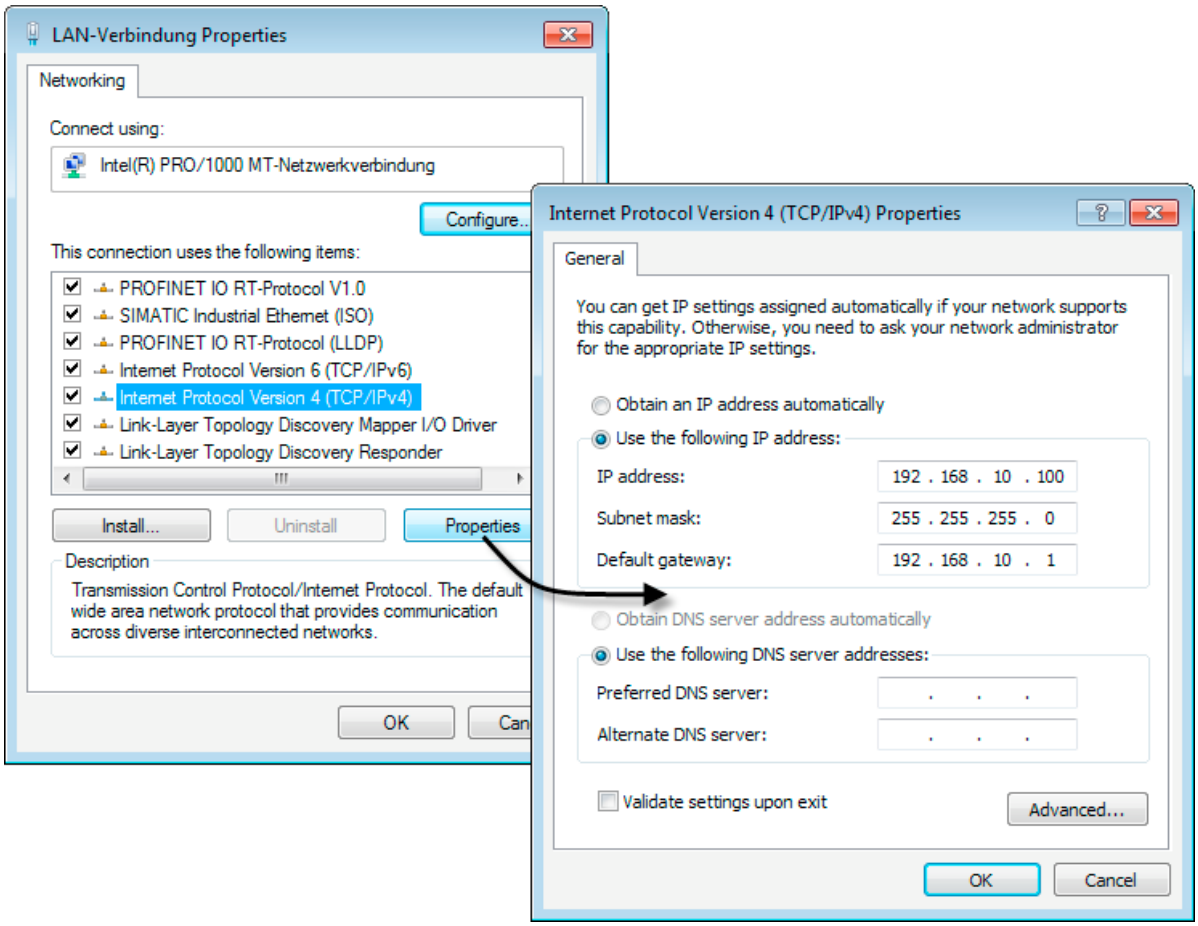
- PC1 utiliza la interfaz externa.
- PC2 utiliza la interfaz interna.

Proceda del siguiente modo en el PC1 y el PC2:

1. Abra el panel de control en el respectivo PC con el siguiente comando de menú:

   Inicio ▸ Panel de control

2. Abra el símbolo "Red y centro de autorización" y, en el menú de navegación que se encuentra a la izquierda, seleccione la opción "Modificar los ajustes del adaptador".
3. Active en el diálogo "Propiedades de la conexión LAN" la casilla de opción "Protocolo Internet versión 4 (TCP/IPv4)" y haga clic en el botón "Propiedades".


LAN-Verbindung Properties
Networking
Connect using:
Intel(R) PRO/1000 MT-Netzwerkverbindung
Configure...
This connection uses the following items:
PROFINET IO RT-Protocol V1.0
SIMATIC Industrial Ethernet (ISO)
PROFINET IO RT-Protocol (LLDP)
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 10 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4. Seleccione en el diálogo "Propiedades del protocolo de Internet versión 4 (TCP/IPv4)" la casilla de verificación "Usar la siguiente dirección IP:" e introduzca en los campos previstos al efecto los valores correspondientes al PC, tomados de la tabla "*Crear configuración IP de los PCs*".

   Cierre los cuadros de diálogo con "Aceptar" y salga del panel de control.

3.3.4 Crear proyecto y módulo

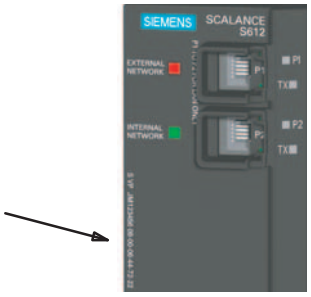
Proceda del siguiente modo:

1. Instala e inicie el software de configuración "Security Configuration Tool" en el PC1.
2. Cree un nuevo proyecto con el siguiente comando de menú:

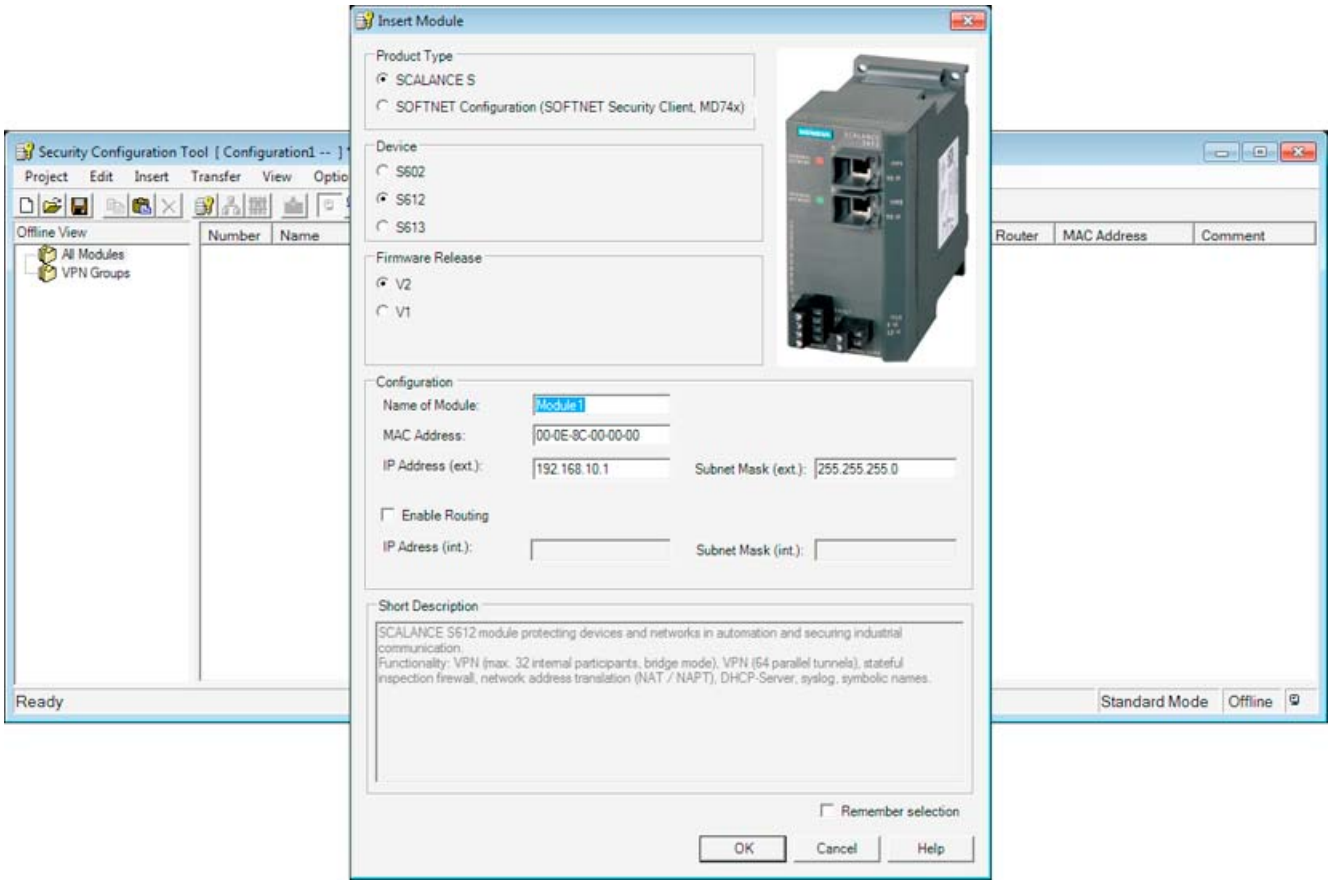
   Project ▸ New

   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted entra aquí se le asigna el papel de un administrador.
3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto crea un nuevo proyecto.
4. Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software". Configure ahora su tipo de producto, el módulo y la versión de firmware.
5. Introduzca en el campo de la "dirección MAC" en la parte de "Configuración" la dirección MAC impresa en la carcasa del módulo en el módulo en el formato preestablecido.

   Encontrará esta dirección en la cara frontal del módulo SCALANCE S (vea la figura)



6. Introduzca también en el formato preestablecido la dirección IP externa (192.168.10.1) y la máscara de subred externa (255.255.255.0), y confirme el diálogo con "OK". De ahí en adelante se incluirá su módulo en la lista de los módulos configurados.



3.3.5 Configurar modo NAT Router

La aplicación más frecuente, en la que todas las estaciones internas envían telegramas a la red externa, ocultando su dirección IP mediante las funciones de NAT, está preconfigurada para el SCALANCE S. Tal como se muestra a continuación, este comportamiento se puede activar haciendo simplemente un clic en el modo Routing.

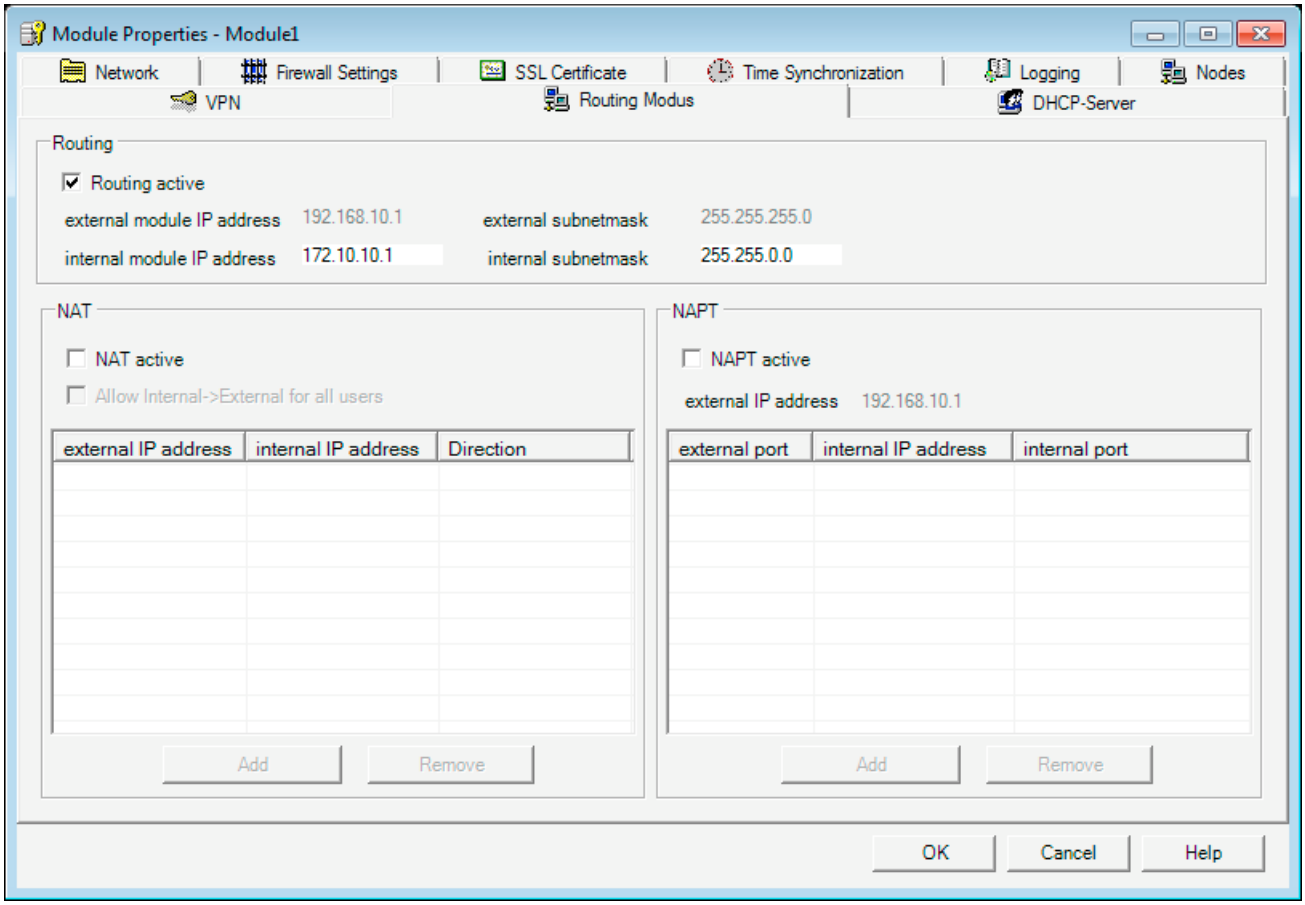
Activación del modo Router - procedimiento:

1. Conmute primero la vista de configuración al Advanced Mode.
2. Seleccione para ello el siguiente comando de menú:

   View ▸ Advanced Mode

3. Haga un doble clic en el módulo SCALANCE S. Con ello se abre el cuadro de diálogo para ajustar las propiedades del módulo.

4. En el cuadro de diálogo visualizado, seleccione la ficha "Routing Modus".



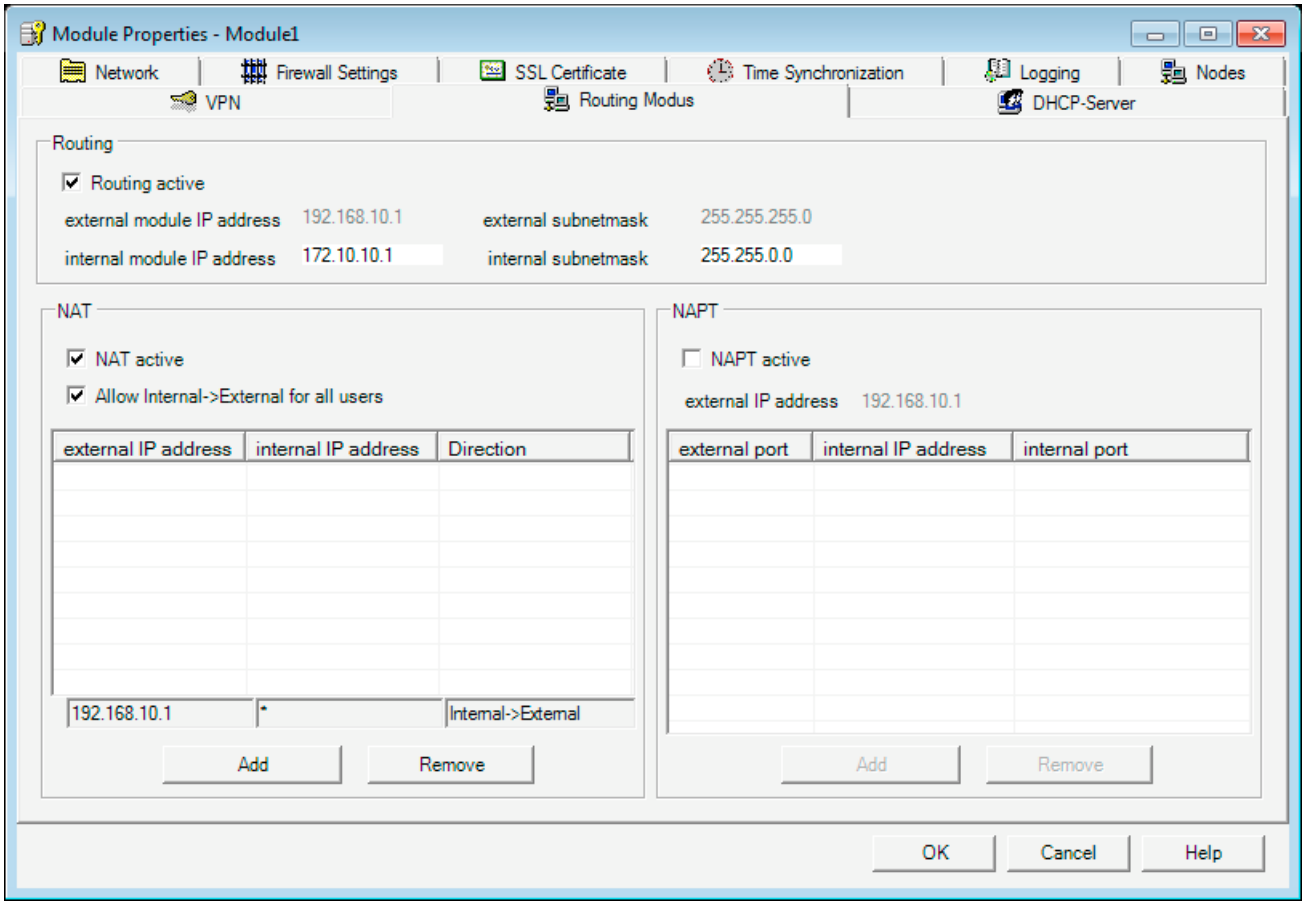
5. Seleccione la opción "active" en el campo de entrada "Routing".
6. Complemente ahora en el campo de entrada "Routing" los datos de dirección para la interfaz del SCALANCE S con la red interna del siguiente modo:
   - Dirección IP del módulo interno: 172.10.10.1
   - Máscara de subred interna: 255.255.255.0

Activación del modo NAT Router para estaciones internas - procedimiento:

Ahora se trata de configurar la conversión de direcciones necesaria para el modo NAT.

1. Seleccione para ello en el campo de entrada "NAT" las dos opciones "NAT active" y "Allow Internal > External for all users".

Puede ver que en el campo de entrada "NAT" se ha completado la lista de conversión de direcciones agregando una entrada al final. La entrada "*" en la columna "internal IP address" representa ahora a todas las estaciones de la red interna.



2. Cierre ahora el cuadro de diálogo con "OK".

Ahora sólo tiene que cuidar de que el firewall permita el paso de telegramas de la red interna hacia la externa.

3.3.6 Configurar firewall

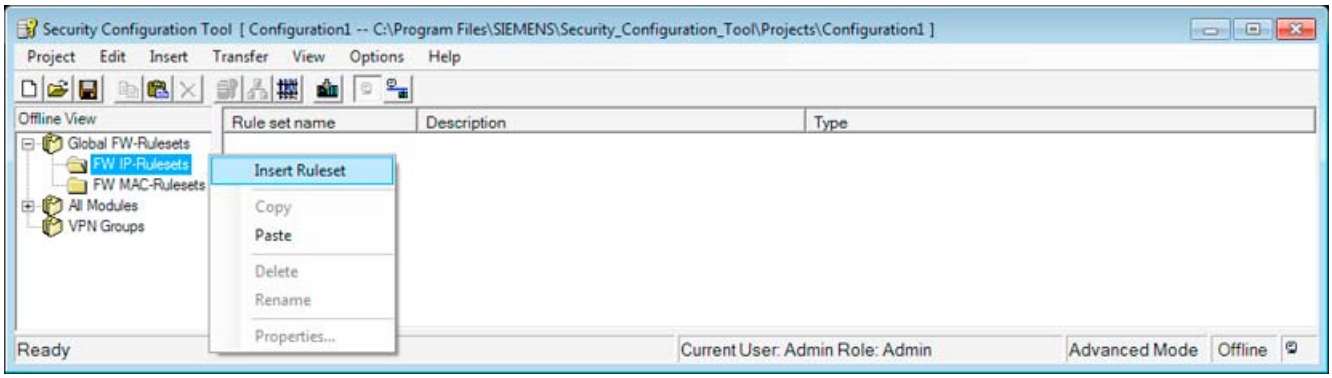
Tiene que definir ahora un bloque de reglas que permita el tráfico de telegramas desde la estación interna (PC2) hacia la estación de la red externa (PC1).

El ejemplo le muestra además cómo puede definir globalmente un bloque de reglas y cómo puede asignarlo a un módulo. Si configura otros módulos en el mismo proyecto, bastará asignar el bloque de reglas definido a los demás módulos por "Drag and Drop"; naturalmente, siempre y cuando se deban aplicar para ellos las mismas reglas.

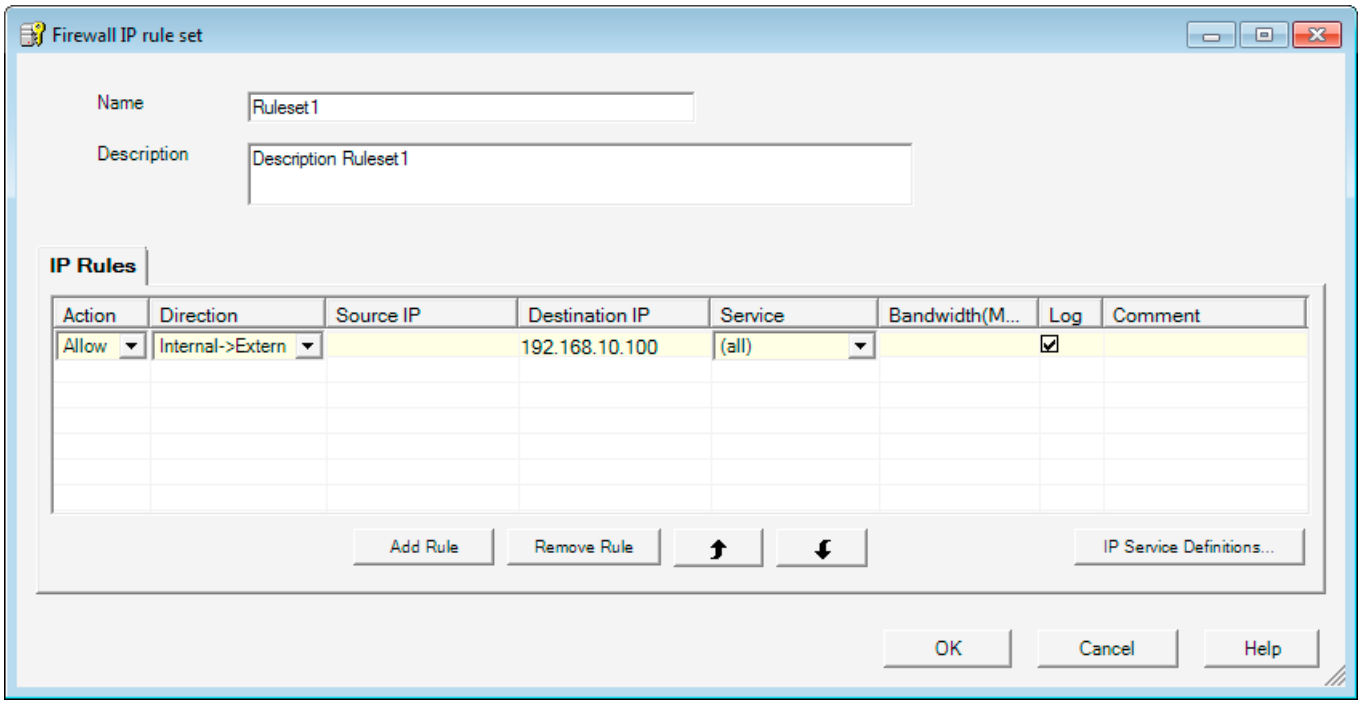
Definición de bloque de reglas global - procedimiento:

1. Abra en el área de navegación el objeto "Global FW Rulesets" y seleccione allí "FW IP Rulesets".
2. Seleccione el siguiente comando con el botón derecho del ratón:

   Insert > Firewall rule set



3. En el cuadro de diálogo presentado, introduzca un bloque de reglas de la siguiente forma:



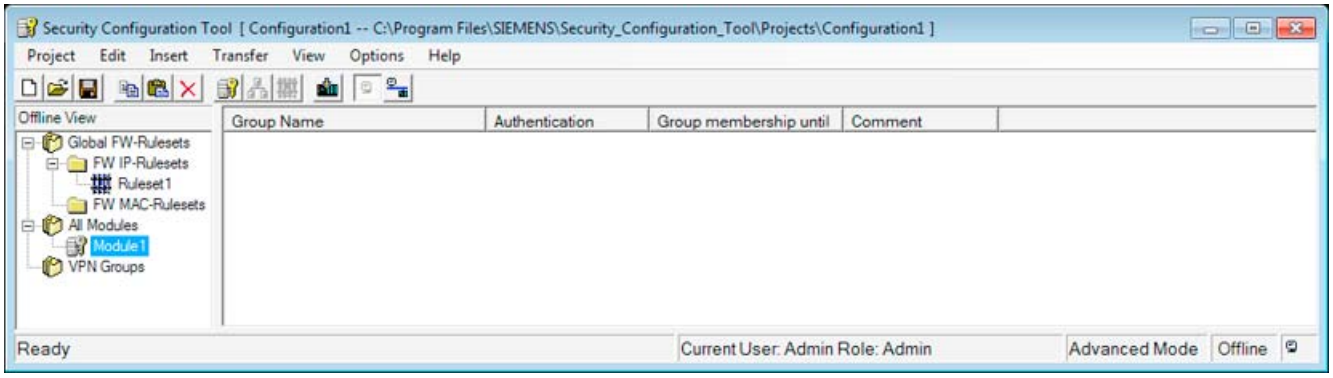
4. Haga clic en la columna "Log", en la fila del nuevo bloque de reglas. Con esto se activa la opción Packet Filter Logging. Entonces se registran los telegramas para los que se apliquen las reglas definidas.

   Este registro lo utilizará en el ejemplo aquí mostrado para el test final de la configuración.

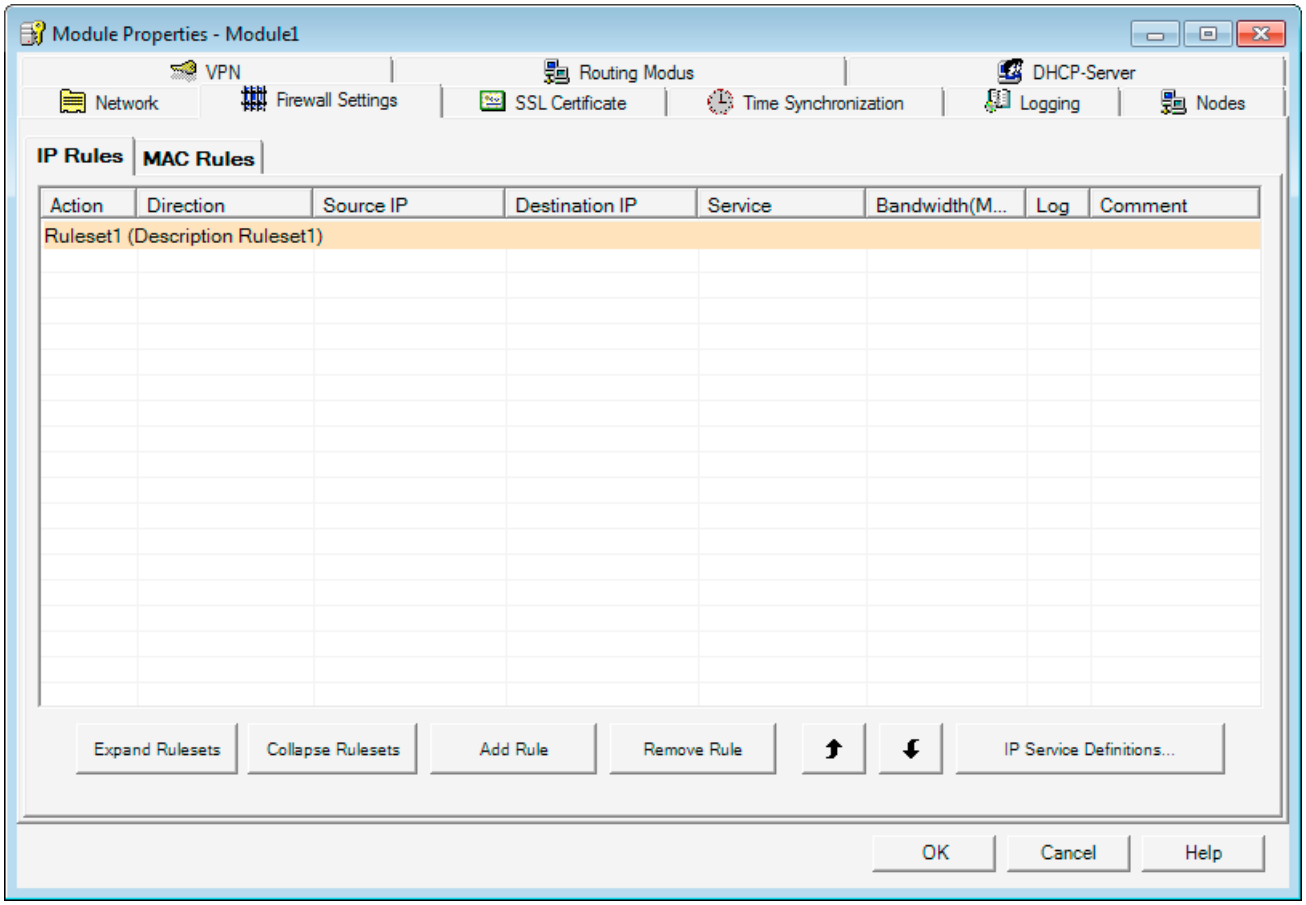
5. Cierre el cuadro de diálogo con "OK".

Asignación de bloque de reglas global - procedimiento:

1. Seleccione en el área de navegación el objeto "Module1" y, manteniendo pulsado el botón izquierdo del ratón, arrástrelo al nuevo bloque de reglas globales de firewall creado.



2. Puede controlar la asignación abriendo de nuevo el cuadro de diálogo para ajuste de las propiedades del módulo y seleccionando allí la ficha "Firewall".



Puede ver que la regla global de firewall se ha archivado allí.

3. Pulsando el botón "Expand Rulesets" puede visualizar el bloque de reglas en detalle.

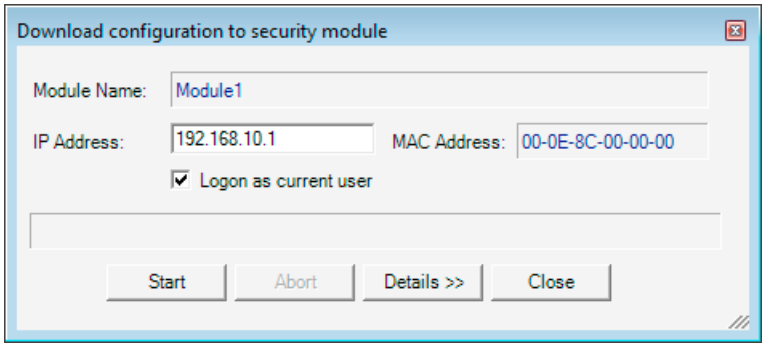
Con esto ha concluido la configuración offline.

3.3.7 Cargar la configuración en SCALANCE S

Proceda del siguiente modo:

1. Seleccione el módulo en el área de contenido.
2. Seleccione el siguiente comando de menú:

   Transfer ▸ To Module...



3. Inicie el proceso de carga con el botón "Start".

Si el proceso de carga se ha concluido sin errores, el SCALANCE S arranca de nuevo automáticamente y se activa la nueva configuración.

Resultado: SCALANCE S en modo productivo

SCALANCE S se encuentra ahora en el modo productivo. Este estado es señalizado por el diodo indicador Fault con luz verde.

Con esto ha terminado la puesta en servicio de la configuración y el SCALANCE S protege ahora, con el firewall instalado, la red interna (PC 2) conforme a la regla configurada: "Allow outgoing IP traffic" de la red interna a la externa.

3.3.8 Probar la función NAT Router (Ping-Test)

¿Cómo se puede probar la función configurada?

La prueba de la función se puede realizar con un comando "ping" tal como se describe a continuación. Para poder reconocer las repercusiones del modo NAT Router, utilice la posibilidad del Packet Filter Logging en la interfaz de firewall.

Recuerde: Al definir la regla global de firewall ha activado ya la opción Packet Filter Logging.

Observación sobre el comando Ping: Como alternativa se pueden utilizar otros programas de comunicación para el test de la configuración.

ATENCIÓN
En caso de Windows, el cortafuegos (firewall) puede estar ajustado como estándar de manera que no puedan pasar comandos PING. Eventualmente tendrá que habilitar los servicios ICMP del tipo Request y Response.

Sección de test 1 - Enviar comando Ping

Pruebe ahora el funcionamiento del modo NAT Router con el tráfico de datos IP de red interna a red externa del siguiente modo:

1. En el PC2, llame en la barra de inicio el siguiente comando de menú:

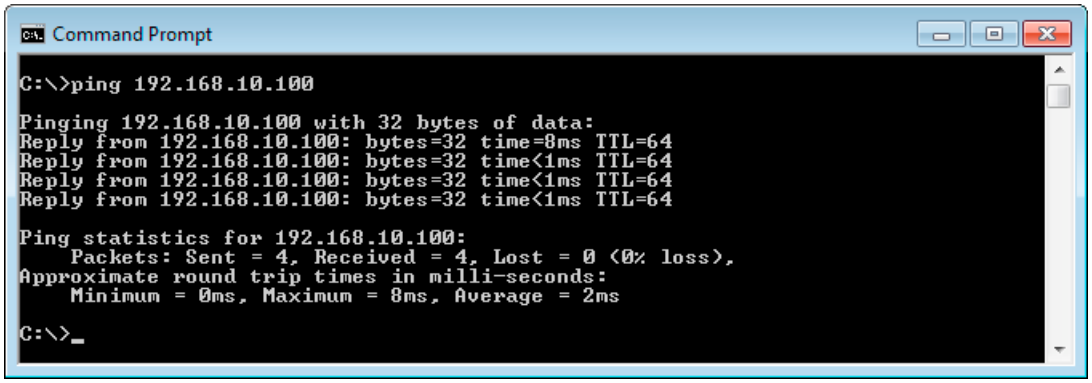
   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

2. Entrada del comando Ping de PC2 a PC1 (dirección IP 192.168.10.100)

   Directamente en la línea de comandos de la ventana presentada "Símbolo del sistema", introduzca en la posición del cursor el siguiente comando:

   ping 192.168.10.100

   Aparecerá entonces el siguiente mensaje: (respuesta positiva del PC1).



Sección de test 2 - Evaluar el resultado

1. Pase ahora al modo online de la Security Configuration Tool. Seleccione para ello el siguiente comando de menú:

   View ▸ Online

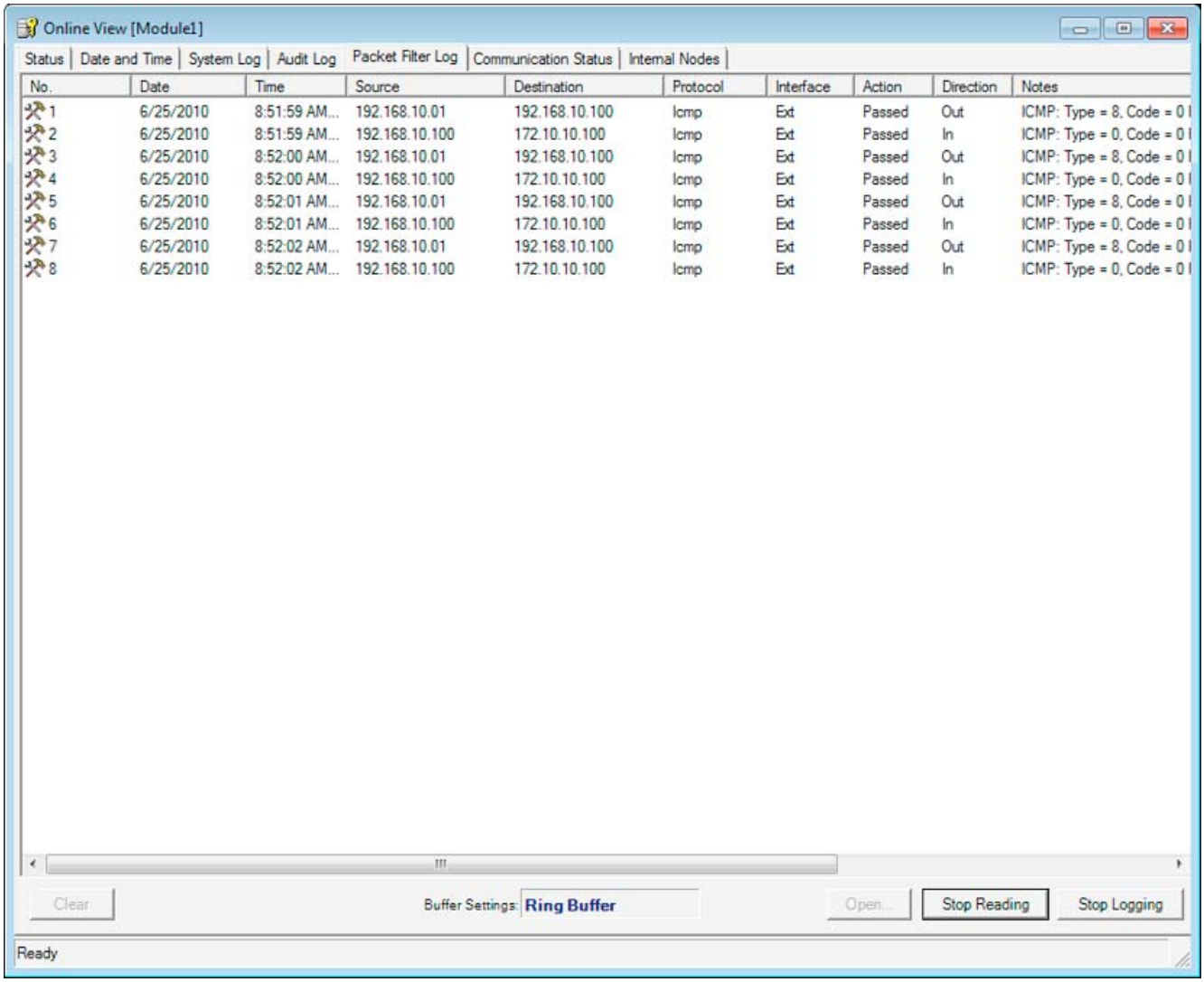
2. Marque el módulo a editar y seleccione, para abrir el cuadro de diálogo online, el comando de menú

   Edit ▸ Online Diagnostics...

   Seleccione la ficha "Packet Filter Log".

3. Accione el botón "Start Reading"
4. Confirme el cuadro de diálogo presentado con "OK".

   Resultado: Las entradas Log se leen del SCALANCE S y se presentan aquí.


Online View [Module1]
Status
Date and Time
System Log
Audit Log
Packet Filter Log
Communication Status
Internal Nodes
No. Date Time Source Destination Protocol Interface Action Direction Notes
1 6/25/2010 8:51:59 AM... 192.168.10.01 192.168.10.100 Icmp Ext Passed Out ICMP: Type = 8, Code = 0
2 6/25/2010 8:51:59 AM... 192.168.10.100 172.10.10.100 Icmp Ext Passed In ICMP: Type = 0, Code = 0
3 6/25/2010 8:52:00 AM... 192.168.10.01 192.168.10.100 Icmp Ext Passed Out ICMP: Type = 8, Code = 0
4 6/25/2010 8:52:00 AM... 192.168.10.100 172.10.10.100 Icmp Ext Passed In ICMP: Type = 0, Code = 0
5 6/25/2010 8:52:01 AM... 192.168.10.01 192.168.10.100 Icmp Ext Passed Out ICMP: Type = 8, Code = 0
6 6/25/2010 8:52:01 AM... 192.168.10.100 172.10.10.100 Icmp Ext Passed In ICMP: Type = 0, Code = 0
7 6/25/2010 8:52:02 AM... 192.168.10.01 192.168.10.100 Icmp Ext Passed Out ICMP: Type = 8, Code = 0
8 6/25/2010 8:52:02 AM... 192.168.10.100 172.10.10.100 Icmp Ext Passed In ICMP: Type = 0, Code = 0
Clear
Buffer Settings: Ring Buffer
Open...
Stop Reading
Stop Logging
Ready

Resultado

En las líneas de salida de la autenticación verá lo siguiente:

- Línea de salida 1

  Las direcciones IP de los telegramas de PC2 a PC1 se muestran en la interfaz con la red externa con la dirección IP externa del módulo SCALANCE S (192.168.10.01). Esto responde a la esperada conversión de direcciones (observación: aquí no se ve la asignación adicional de puerto).

- Línea de salida 2

Los telegramas de respuesta se muestran con la dirección de destino de la estación de la subred interna (PC2: 172.10.10.100). Con esto puede reconocer que se ha producido la conversión de direcciones, antes de que el telegrama de respuesta atraviese el firewall.

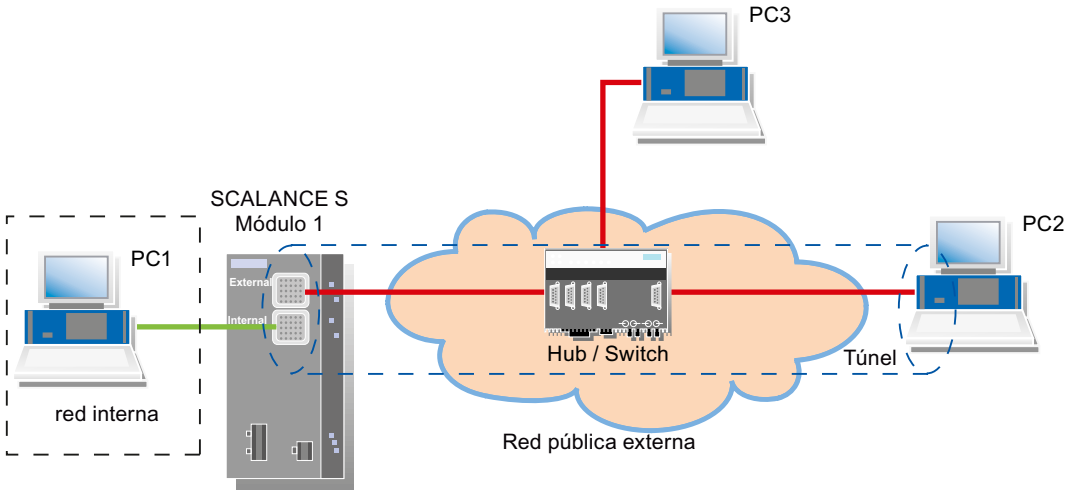
3.4 Ejemplo 4: Acceso remoto - Ejemplo de túnel VPN con SCALANCE S612 / S613 y SOFTNET Security Client

3.4.1 Resumen

En este ejemplo se configura la función Túnel VPN en la vista de configuración "Standard Mode". Un SCALANCE S y el SOFTNET Security Client constituyen en este ejemplo los dos puntos finales del túnel para la conexión de túnel protegida a través de una red pública.

Con esta configuración se consigue que el tráfico IP entre dos interlocutores autorizados sólo sea posible a través de las conexiones de túnel VPN establecidas.

Construcción de la red de test



- Red interna - conexión a SCALANCE S Port 2 (puerto "Internal Network")

  En la estructura de test, en la red interna un nodo de red se realiza por medio de un PC que está conectado al puerto "Internal Network" (Port 2, verde) de un módulo SCALANCE S.

  – PC1: representa a una estación participante en la red interna

  – SCALANCE S Module 1: Módulo SCALANCE S para protección de la red interna

- Red externa, pública - conexión a SCALANCE S Port 1 (puerto "External Network")

  La red externa pública se conecta al puerto "External Network" (Port 1, rojo) de un módulo SCALANCE S.

  – PC2: PC con el software de configuración Security Configuration Tool y el software SOFTNET Security Client para el acceso VPN seguro a la red interna

  – PC3: PC de test para la sección de test 2

Nota

En el ejemplo, en representación de una red WAN externa pública se recurre a una red local para explicar los aspectos básicos del funcionamiento correspondiente.

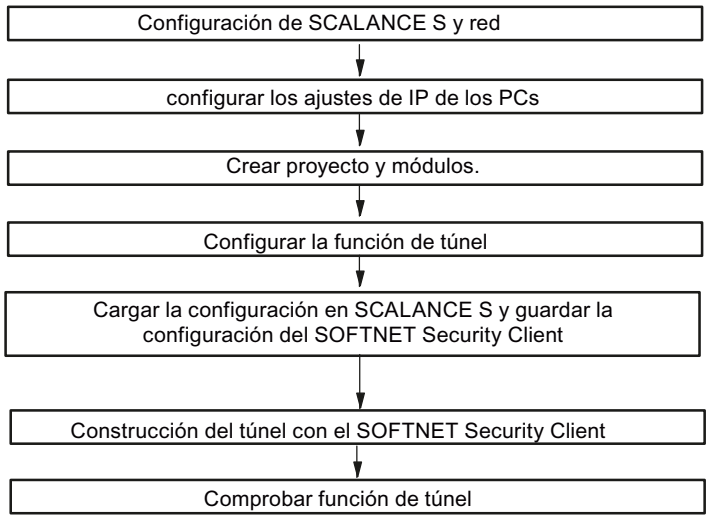
En los lugares correspondientes se dan explicaciones relativas al uso de una WAN.

Dispositivos/componentes necesarios:

Utilice los siguientes componentes para el montaje:

- 1 módulo SCALANCE S (opcional: un riel de perfil de sombrero correspondientemente instalado, con material de montaje);
- 1 alimentación eléctrica de 24V con conexiones de cables y conectores de bloque de bornes;
- 1 PC en el que esté instalada la herramienta de configuración "Security Configuration Tool" y el VPN-Client "SOFTNET Security Client";
- 1 PC en la red interna, para test de la configuración;
- 1 PC en la red externa, para test de la configuración;
- 1 hub o switch de red para el establecimiento de conexiones de red con el módulo SCALANCE S así como el PC;
- los necesarios cables de red, cables TP (Twisted Pair) según el estándar IE FC RJ45 para Industrial Ethernet.

Los pasos siguientes, en síntesis:


Configuración de SCALANCE S y red
configurar los ajustes de IP de los PCs
Crear proyecto y módulos.
Configurar la función de túnel
Cargar la configuración en SCALANCE S y guardar la configuración del SOFTNET Security Client
Construcción del túnel con el SOFTNET Security Client
Comprobar función de túnel

3.4.2 Instalar el SCALANCE S y la red

Procedimiento a seguir:

1. Saque primero el SCALANCE S de su embalaje y compruebe si está en perfecto estado.
2. Conecte la alimentación de tensión al módulo SCALANCE S.

Resultado: Tras conectar la tensión de servicio brilla el diodo Fault (F) con luz amarilla.

⚠ ADVERTENCIA

El equipo SCALANCE S está previsto para funcionar con baja tensión de seguridad. En consecuencia, a las conexiones de alimentación sólo se deben conectar bajas tensiones de seguridad (SELV) según IEC950/EN60950/ VDE0805.

La fuente de alimentación utilizada para el SCALANCE S tiene que ser del tipo NEC Class 2 (gama de tensión 18-32 V, consumo de corriente aprox. 250 mA).

Para el montaje y la conexión de los módulos SCALANCE S, tenga en cuenta el capítulo "Propiedades del producto y puesta en servicio".

1. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45):

– Conecte el PC1 al puerto 2 del Module 1.
– Conecte el puerto 1 del Module 1 al hub/switch.
– Conecte también PC2 y PC3 al hub/switch.

2. Encienda los PCs participantes.

Nota

Para el uso de una WAN como red externa pública, las conexiones con el hub/switch se tienen que reemplazar por las conexiones con la red WAN (acceso a Internet).

ATENCIÓN

Las conexiones de Ethernet en Port 1 y Port 2 son tratadas de forma diferente por el SCALANCE S, por lo que no se deben confundir al establecer la conexión con la red de comunicación:

- Port 1 - "External Network"
  conector hembra RJ45 superior, marca roja = área de red no protegida;
- Port 2 - "Internal Network"
  conector hembra RJ45 inferior, marca verde = red protegida por SCALANCE S

Si se permutan los puertos, el equipo pierde su función de protección.

3.4.3 Preparar ajustes IP de los PCs

Los PCs deberían tener los siguientes ajustes de dirección IP para el test:

PC	Dirección IP	Máscara de subred	Gateway estándar
PC1	192.168.0.1	255.255.255.0	192.168.0.201
PC2	191.0.0.2	255.255.0.0	191.0.0.201
PC3	191.0.0.3	255.255.0.0	191.0.0.201

Como Gateway estándar se han de indicar las direcciones IP que se asignan al módulo SCALANCE S en la configuración subsiguiente para la interfaz interna y la externa:

- PC1 utiliza la interfaz interna.
- PC2 y PC3 utilizan la interfaz externa.

Nota

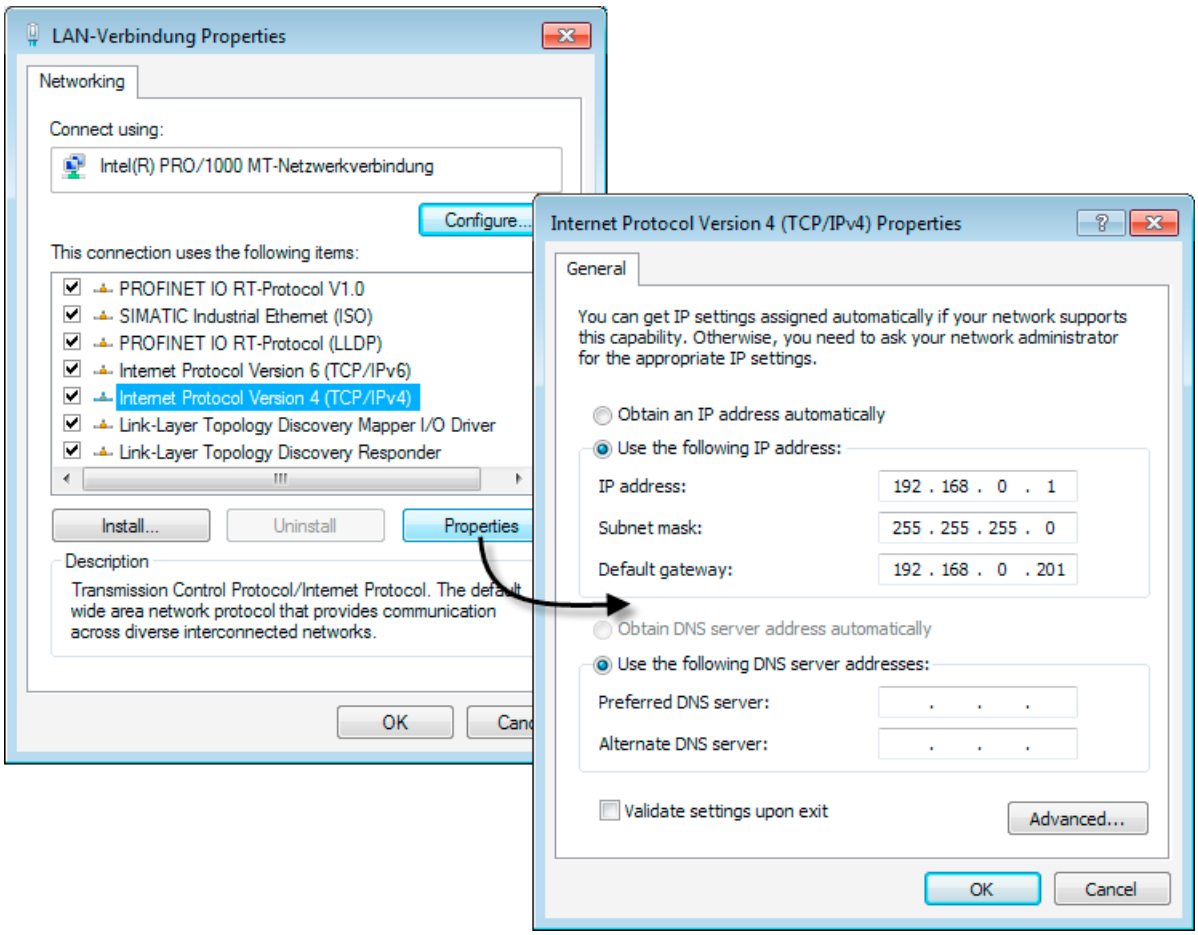
Para el uso de una WAN como red externa pública se tienen que preparar en PC2 y PC3 los respectivos ajustes IP para la conexión con la red WAN (Internet).

Proceda del siguiente modo para PC1, PC2 y PC3:

1. Abra el panel de control en el respectivo PC con el siguiente comando de menú:

Inicio ▸ Panel de control

2. Abra el símbolo "Red y centro de autorización" y, en el menú de navegación que se encuentra a la izquierda, seleccione la opción "Modificar los ajustes del adaptador".
3. Active en el diálogo "Propiedades de la conexión LAN" la casilla de opción "Protocolo Internet versión 4 (TCP/IPv4)" y haga clic en el botón "Propiedades".


LAN-Verbindung Properties
Networking
Connect using:
Intel(R) PRO/1000 MT-Netzwerkverbindung
Configure...
This connection uses the following items:
PROFINET IO RT-Protocol V1.0
SIMATIC Industrial Ethernet (ISO)
PROFINET IO RT-Protocol (LLDP)
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 201
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4. Seleccione en el diálogo "Propiedades del protocolo de Internet versión 4 (TCP/IPv4)" la casilla de verificación "Usar la siguiente dirección IP:" e introduzca en los campos previstos al efecto los valores correspondientes al PC, tomados de la tabla "*Crear configuración IP de los PCs*".

   Cierre los cuadros de diálogo con "Aceptar" y salga del panel de control.

3.4.4 Crear proyecto y módulos

Procedimiento a seguir:

1. Inicie el software de configuración Security Configuration Tool en PC2.
2. Cree un nuevo proyecto con el siguiente comando de menú:

   Project ▸ New

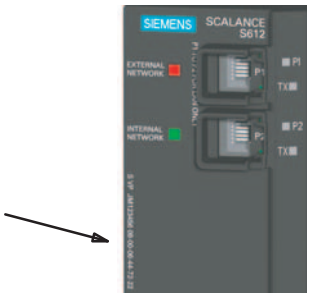
   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted entra aquí se le asigna automáticamente el papel de un administrador.
3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto crea un nuevo proyecto.
4. Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software". Configure ahora el tipo de producto, el módulo y la versión de firmware, cerrando al final el diálogo pulsando "OK".
5. Cree un segundo módulo con el siguiente comando de menú:

   Insert ▸ Module

   Configure ahora el tipo de producto "SOFTNET Configuration", el módulo "SOFTNET Security Client" y la versión de firmware de su SOFTNET Security Client Version, cerrando al final el diálogo pulsando "OK".

   A este módulo se le asigna automáticamente un nombre según lo ajustado previamente para el proyecto.
6. Haga clic en el área de navegación en "All Modules" y a continuación en el área de contenido, en la línea con "Module 1".
7. Haga clic ahora en la columna "MAC Address" e introduzca ésta en el formato predeterminado.

   Encontrará esta dirección en la cara frontal del módulo SCALANCE S (véase la figura)



8. Haga clic ahora en la columna "IP Address ext.", introduzca ésta en el formato predeterminado y adapte también la máscara de subred.
   Para Module1: Dirección IP: 191.0.0.201, Máscara de subred: 255.255.0.0

   Nota

   Para el uso de una WAN como red externa pública, introduzca como "IP Adress ext." su dirección IP estática recibida del proveedor, a través de la que luego se podrá acceder al módulo SCALANCE S en la WAN (Internet).

   Para que el módulo SCALANCE S pueda enviar paquetes a través de la WAN (Internet), tiene que introducir su router DSL como "Default Router".

   Si utiliza un DSL-Router como Internet Gateway, tiene que activar en él al menos los puertos siguientes:

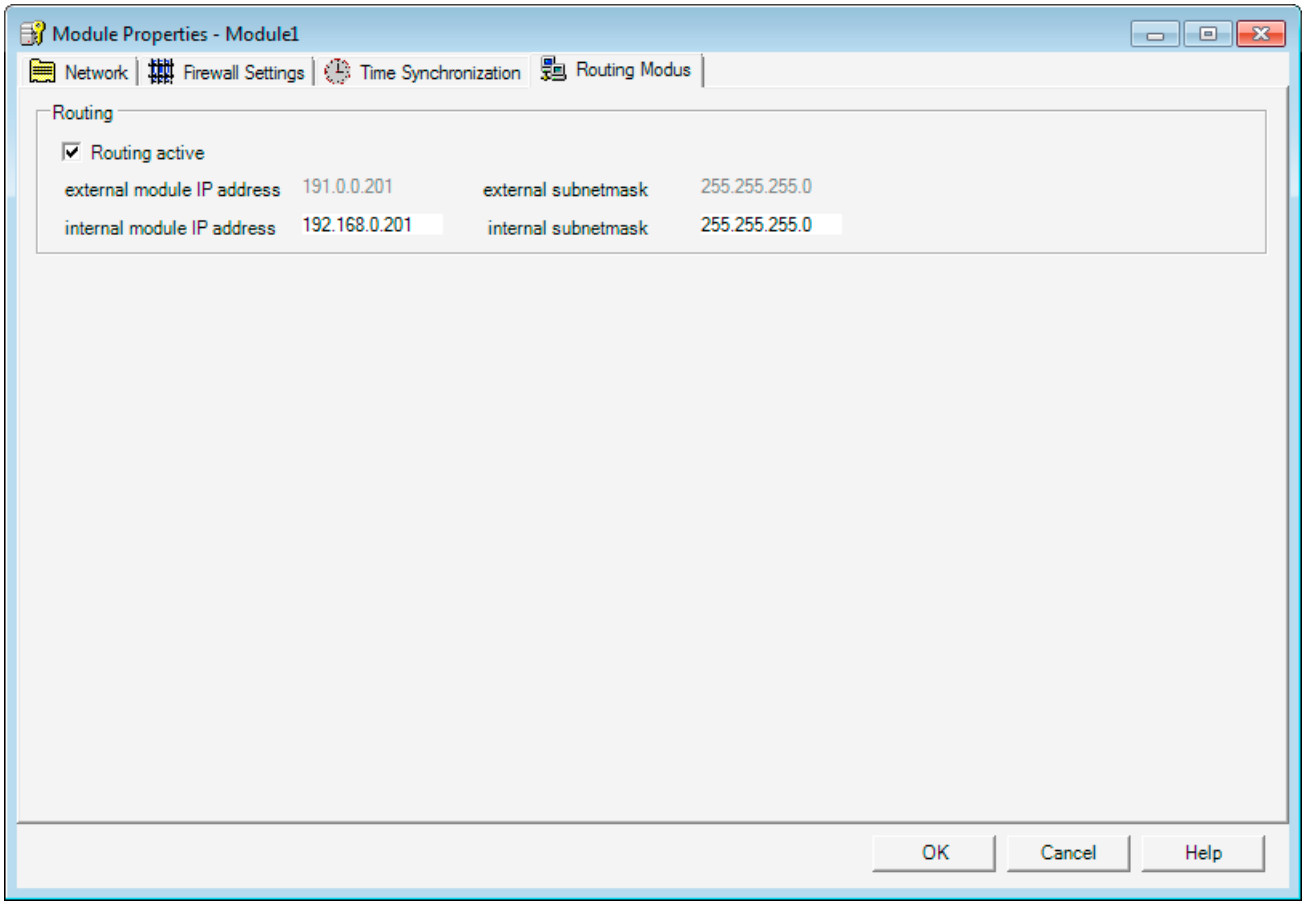
   • Port 500 (ISAKMP)

   • Port 4500 (NAT-T)

   Si se descargan configuraciones (no a través de un túnel activo) se tiene que activar además el Port 443 (HTTPS).

9. Abra ahora el menú de propiedades del "Module 1" seleccionando la entrada, pulsando el botón derecho del ratón y seleccionando el tópico de menú "Propiedades…".

10. Active ahora, según se muestra en la vista siguiente, en la ficha "Routing Modus" el modo Routing, introduzca la dirección IP interna (192.168.0.201) y la máscara de subred (255.255.255.0) del módulo SCALANCE S y confirme con "OK".

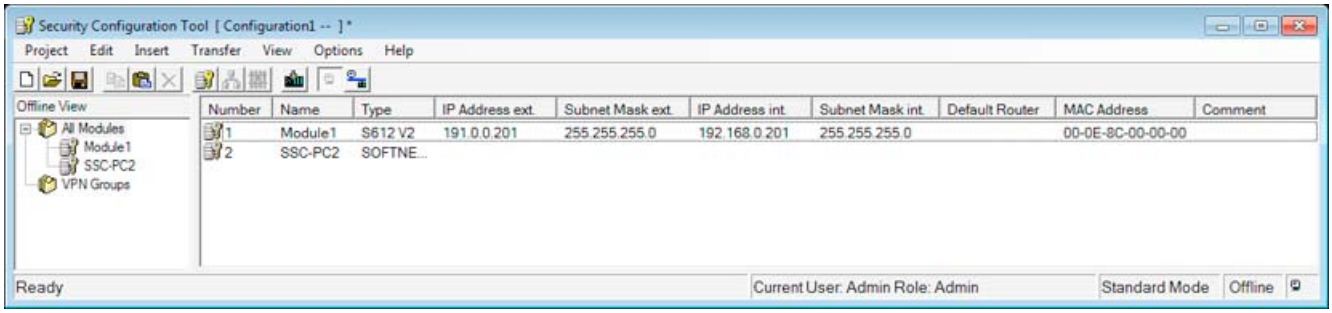


11. Haga clic en el área de navegación en "All Modules" y a continuación en el área de contenido, en la línea con "Module 2".

12. Haga clic en la columna "Name" e introduzca el nombre "SSC-PC2".

El SOFTNET Security Client no necesita más ajustes.

Su vista debería ser ahora similar a la de la ilustración siguiente.


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
SSC-PC2
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 191.0.0.201 255.255.255.0 192.168.0.201 255.255.255.0 00-0E-8C-00-00-00
2 SSC-PC2 SOFTNE...
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

3.4.5 Configurar conexión túnel

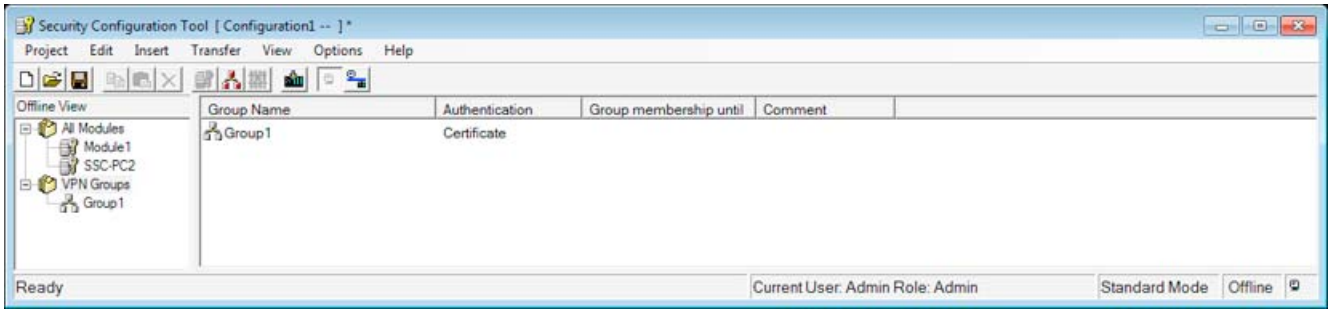
Un SCALANCE S y el SOFTNET Security Client pueden crear exactamente un túnel IPSec para la comunicación segura si están asignados a un mismo grupo en el proyecto.

Procedimiento a seguir:

1. Seleccione en el área de navegación "All Groups" y cree un nuevo grupo con el siguiente comando de menú:

   Insert ▸ Group

   Este grupo recibe automáticamente el nombre "Group 1".



2. Seleccione en el área de contenido el módulo de SCALANCE S "Module 1" y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora a ese grupo o bien es miembro de ese grupo.

   El color del símbolo de llave del icono de módulo cambia ahora de gris a azul.

3. Seleccione en el área de contenido el módulo SOFTNET Security Client y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora también a ese grupo.

4. Guarde ahora este proyecto con el siguiente comando de menú, bajo un nombre apropiado:

   Project ▸ Save As…

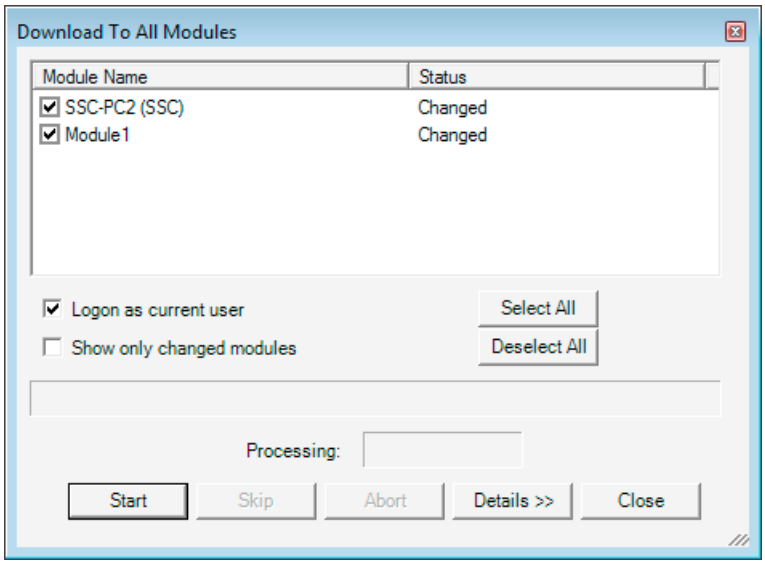
Con esto ha terminado la configuración de la conexión de túnel.

3.4.6 Cargar la configuración en SCALANCE S y guardar la configuración de SOFTNET Security Client

Procedimiento a seguir:

1. Llame el siguiente cuadro de diálogo con el comando aquí indicado:

   Transfer ▸ To All Modules…



2. Inicie el proceso de carga con el botón "Start".
3. Guarde el archivo de configuración "Nombredeproyecto.sscPC2.dat" en su directorio del proyecto y asigne una contraseña como clave privada del certificado.

Si el proceso de carga se ha concluido sin errores, el SCALANCE S arranca de nuevo automáticamente y se activa la nueva configuración.

Resultado: SCALANCE S en modo productivo

SCALANCE S se encuentra ahora en el modo productivo. Este estado es señalizado por el diodo Fault con luz verde.

Con esto ha concluido la puesta en servicio de la configuración y el módulo SCALANCE S y el SOFTNET Security Client pueden crear un túnel de comunicación a través del que se pueden comunicar de forma segura los nodos de las redes internas con PC2.

Nota

Para el uso de una WAN como red externa pública, no se puede configurar un módulo SCALANCE S con la configuración de fábrica a través de la red WAN. Configure en este caso el módulo SCALANCE S a partir de la red interna.

3.4.7 Formación de túnel con el SOFTNET Security Client

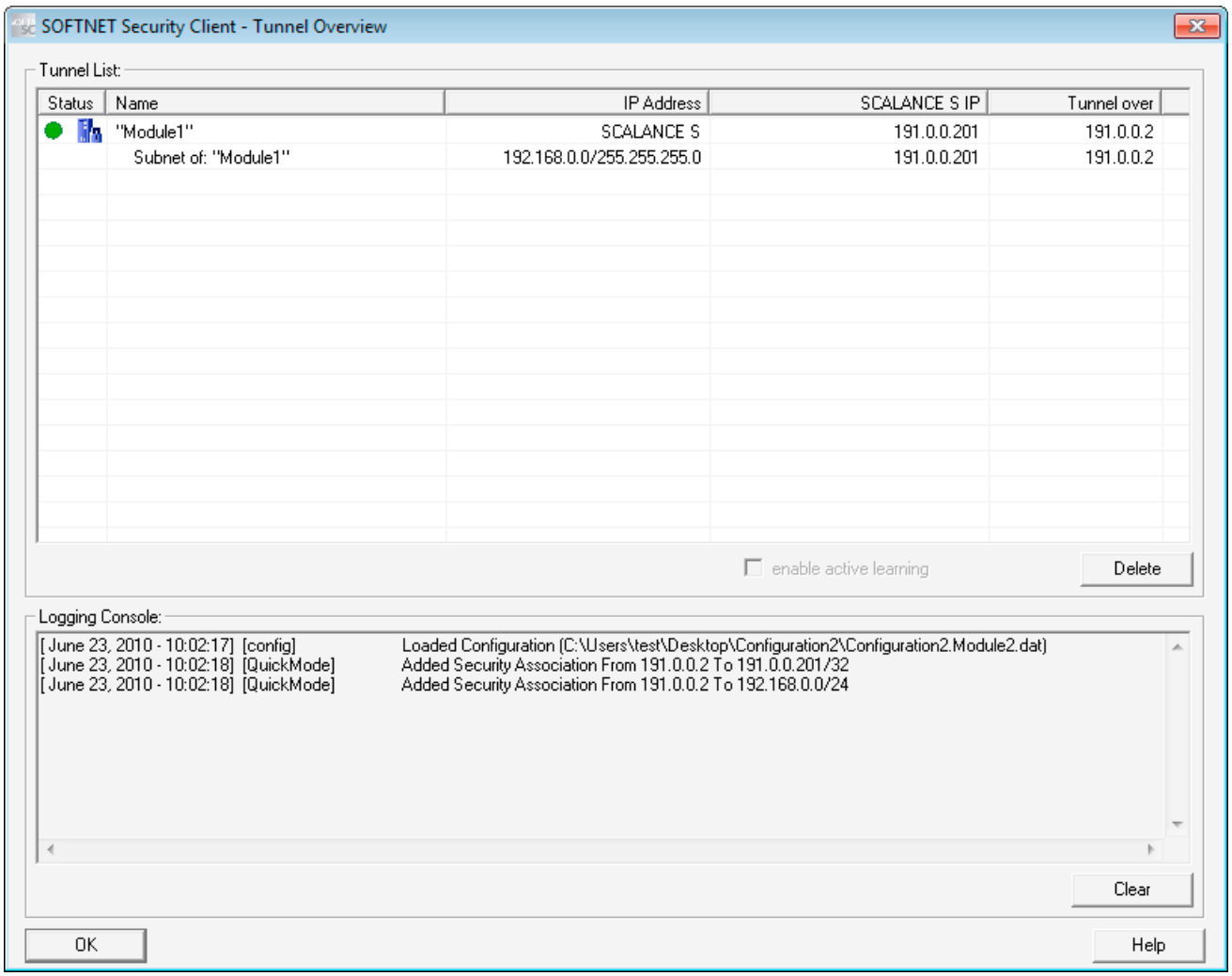
Procedimiento a seguir:

1. Inicie el SOFTNET Security Client en PC2.
2. Pulse el botón "Load Configuration", cambie a su directorio del proyecto y cargue el archivo de configuración "Nombredeproyecto.SSC-PC2.dat".
3. Introduzca la contraseña para la contraseña privada del certificado y confirme con "Next".
4. Confirme el diálogo "Activate static configured members?" con "Yes".
5. Accione el botón "Tunnel Overview"

Resultado: conexión de túnel activa

Se ha establecido el túnel entre SCALANCE S y SOFTNET Security Client. Este estado operativo se señaliza con un círculo verde en la entrada "Module1".

En la consola de Log de la vista del túnel del SOFTNET Security Client aparecen algunas respuestas de su sistema respecto a cómo se ha desarrollado el intento de conexión y sobre si se han establecido directivas para su conexión de comunicación.



Con esto ha concluido la puesta en servicio de la configuración y el módulo SCALANCE S y el SOFTNET Security Client pueden crear un túnel de comunicación a través del que se pueden comunicar de forma segura los nodos de la red interna y PC2.

3.4.8 Probar la función túnel (Ping-Test)

¿Cómo se puede probar la función configurada?

La prueba de la función se puede realizar con un comando "ping" tal como se describe a continuación.

Como alternativa se pueden utilizar otros programas de comunicación para el test de la configuración.

ATENCIÓN
En caso de Windows, el cortafuegos (firewall) puede estar ajustado como estándar de manera que no puedan pasar comandos PING. Eventualmente tendrá que habilitar los servicios ICMP del tipo Request y Response.

Sección de test 1

Compruebe ahora el funcionamiento de la conexión de túnel establecida entre PC1 y PC2 del siguiente modo:

1. En el PC2, llame en la barra de inicio el siguiente comando de menú:

   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

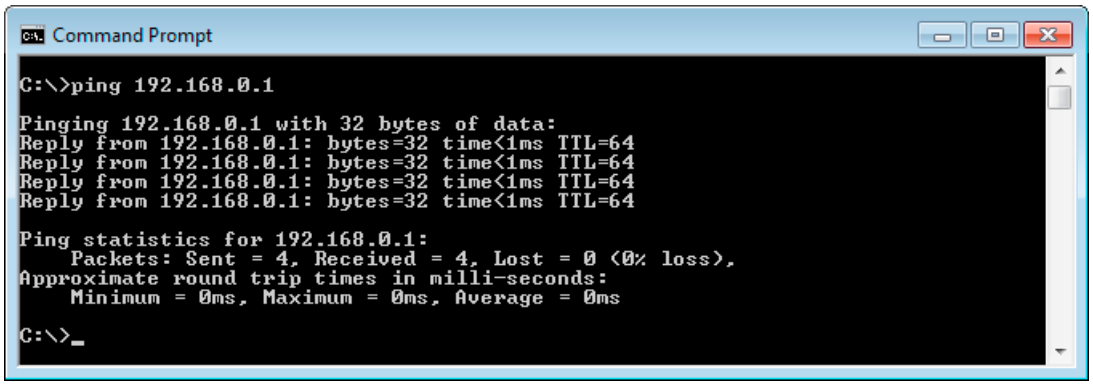
2. Entrada del comando Ping de PC2 a PC1 (dirección IP 192.168.0.1).

   Directamente en la línea de comandos de la ventana que aparece "Símbolo del sistema", introduzca en la posición del cursor el comando

   ping 192.168.0.1

   .

Aparecerá entonces el siguiente mensaje: (respuesta positiva del PC1).



Resultado

Cuando los telegramas IP llegan al PC1, la "estadística Ping" muestra para 192.168.0.1 lo siguiente:

- Enviado = 4
- Recibido = 4
- Perdido = 0 (0% pérdida)

Dado que no estaba permitida ninguna otra comunicación, esto telegramas sólo se pueden haber transportado por el túnel VPN.

Sección de test 2

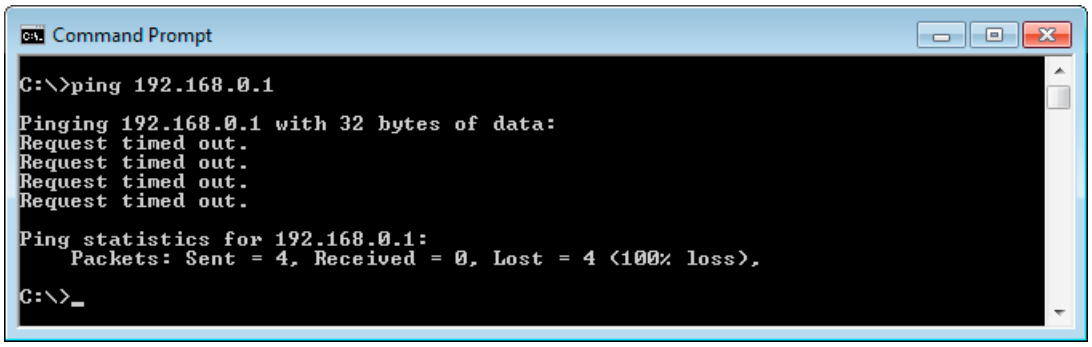
Repita ahora el test emitiendo un comando ping desde el PC3.

1. En el PC3, llame en la barra de inicio el siguiente comando de menú:

   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

2. Emita de nuevo el mismo comando ping (**ping 192.168.0.1**) en la ventana del símbolo del sistema de PC3.

Aparecerá entonces el siguiente mensaje: (ninguna respuesta del PC1).


Command Prompt
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

Resultado

Los telegramas IP del PC3 no pueden llegar al PC1, ya que no hay configurada ninguna comunicación túnel entre estos equipos ni tampoco se permite el tráfico de datos IP normal.

Esto se indica en la "estadística Ping" para 192.168.0.1 del siguiente modo:

- Enviado = 4
- Recibido = 0
- Perdido = 4 (100% pérdida)

3.5 Ejemplo 5: Acceso remoto - ejemplo de túnel VPN con MD741-1 y SOFTNET Security Client

3.5.1 Sinopsis

En este ejemplo se configura la función Túnel VPN en la vista de configuración "Advanced Mode". Un MD741-1 y el SOFTNET Security Client forman los dos puntos finales del túnel para la conexión de túnel segura a través de una red pública.

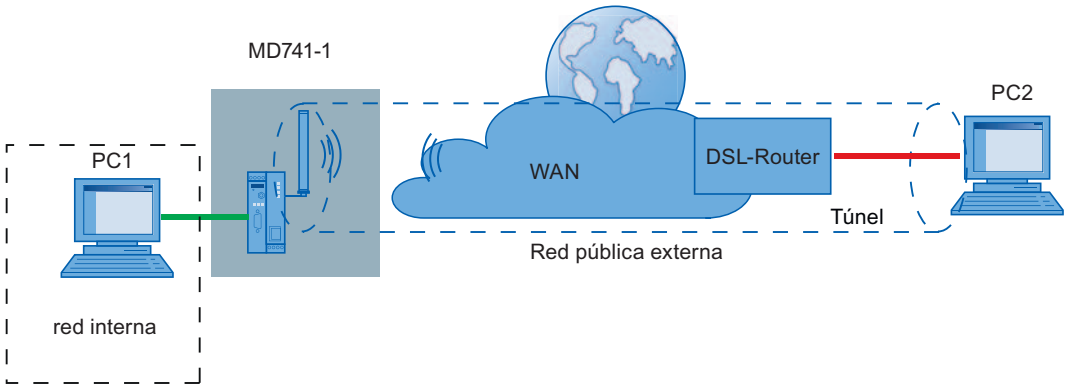
Con esta configuración se consigue que el tráfico IP entre dos interlocutores autorizados sólo sea posible a través de la conexión de túnel VPN establecida.

Nota

Para la configuración de este ejemplo es obligatoriamente necesario tener a disposición una dirección IP pública, no-modificable, para la tarjeta SIM del MD741-1 del propio proveedor (proveedor de teléfono móvil), a la que no se pueda acceder a través de internet.

(Opcionalmente también se puede utilizar una dirección DynDNS para el MD741-1.)

Configuración de la red de test:



- Red interna - conexión a MD741-1 Port X2 ("Internal Network")

  En la configuración de test, en la red interna cada nodo de red se realiza por medio de un PC que está conectado al puerto "Internal Network" (Port X2) de un módulo MD741-1.

  – PC1: representa a una estación de la red interna

  – MD741-1: MD741-1 Módulo para la protección de la red interna

  Red pública externa - conexión a través de la antena MD741-1 ("External Network")

  La red pública externa es una red GSM o de telefonía móvil, que puede ser seleccionada por el abonado del proveedor (de telefonía móvil) y se alcanza a través de la antena del módulo MD741-1.

  – PC2: PC con elsoftware de configuración Security Configuration Tool y el software SOFTNET Security Client para el acceso VPN seguro a la red interna

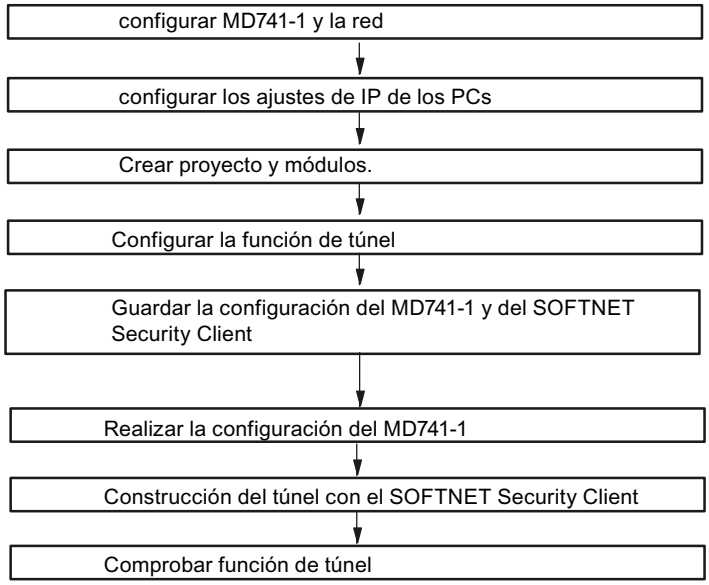
Dispositivos/componentes necesarios:

Utilice los siguientes componentes para el montaje:

- 1x módulo MD741-1 con tarjeta SIM, (opcional: un riel de perfil de sombrero correspondientemente instalado, con material de montaje);
- 1x fuente de alimentación de 24V con conector de cable y enchufe para bloque de bornes;

- 1x PC en el cual va instalada la herramienta de configuración "Security Configuration Tool" y el cliente VPN "SOFTNET Security Client";
- 1x PC en la red interna, del MD741-1 con un navegador para la configuración del MD741-1 y el test de la configuración;
- 1x router DSL (conexión a internet para el PC con el cliente VPN (ISDN, DSL, UMTS, etc.))
- Los cables de red, cables TP (Twisted Pair) necesarios según el estándar IE FC RJ45 para Industrial Ethernet.

Los pasos siguientes, en síntesis


configurar MD741-1 y la red
configurar los ajustes de IP de los PCs
Crear proyecto y módulos.
Configurar la función de túnel
Guardar la configuración del MD741-1 y del SOFTNET Security Client
Realizar la configuración del MD741-1
Construcción del túnel con el SOFTNET Security Client
Comprobar función de túnel

3.5.2 configurar MD741-1 y la red

Procedimiento a seguir:

1. Saque primero el aparato MD741-1 de su embalaje y compruebe si está en perfecto estado.
2. Siga la puesta en servicio "paso a paso" descrita en el manual de sistema MD741-1 hasta llegar al punto en el que deberá configurar según sus requisitos. Utilice para ello PC1, Configuración del MD741, véase el capítulo Realizar la configuración del MD741-1 (Página 96).

3. Establezca las conexiones físicas de red enchufando los conectores de los cables de red en los puertos previstos al efecto (conectores hembra RJ45):
   - Conecte PC1 con el puerto X2 ("red interna") del MD741-1
   - Conecte PC2 con el DSL-Router
4. Ponga en marcha los PCs implicados.

3.5.3 Configurar los ajustes de IP de los PCs

Los PCs deberían tener los siguientes ajustes de dirección IP para el test:

PC	Dirección IP	Máscara de subred	Gateway estándar
PC1	192.168.1.101	255.255.255.0	192.168.1.1
PC2	192.168.2.202	255.255.255.0	192.168.2.1

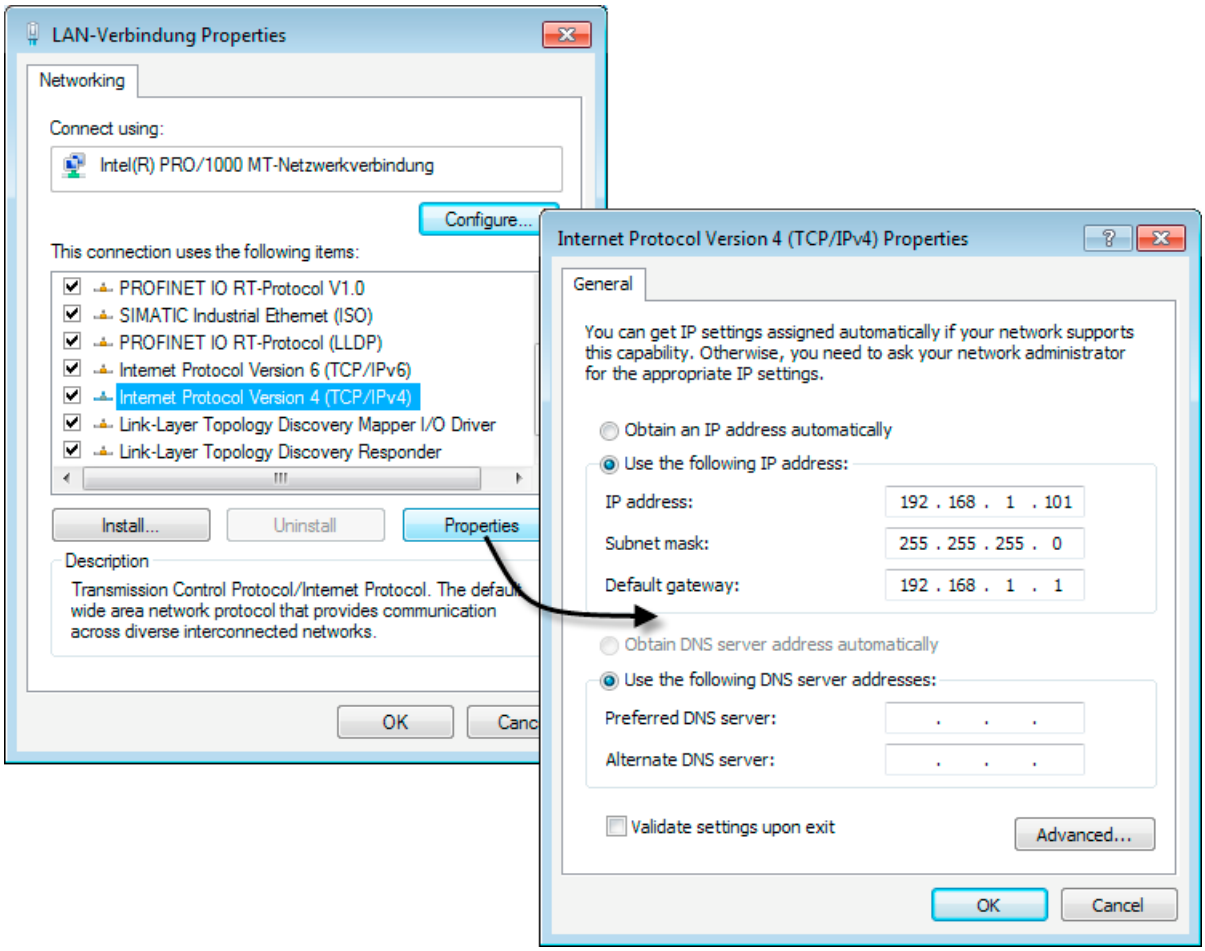
Como gateway estándar para PC1 se ha de indicar la dirección IP que se asigne al módulo MD741-1 (para la interfaz de red interna) en la siguiente configuración. Para PC2, indique la dirección IP del DSL-Router (para la interfaz de red interna).

Con PC1 y PC2 proceda en cada caso de la siguiente manera para abrir las conexiones de red en el PC correspondiente:

1. Abra el panel de control en el respectivo PC con el siguiente comando de menú:

   Inicio ▸ Panel de control
2. Abra el icono "Red y centro de autorización".

3. Active en el diálogo "Propiedades de la conexión LAN" la casilla de opción "Protocolo Internet versión 4 (TCP/IPv4)" y haga clic en el botón "Propiedades".


LAN-Verbindung Properties
Networking
Connect using:
Intel(R) PRO/1000 MT-Netzwerkverbindung
Configure...
This connection uses the following items:
PROFINET IO RT-Protocol V1.0
SIMATIC Industrial Ethernet (ISO)
PROFINET IO RT-Protocol (LLDP)
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default
wide area network protocol that provides communication
across diverse interconnected networks.
OK
Canc
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 101
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4. Seleccione en el diálogo "Propiedades del protocolo de Internet versión 4 (TCP/IPv4)" la casilla de verificación "Usar la siguiente dirección IP:" apagado. Introduzca ahora en los campos previstos al efecto los valores correspondientes al PC, tomados de la tabla "*Crear configuración IP de los PCs*".

   Cierre los cuadros de diálogo con "Aceptar" y salga del panel de control.

3.5.4 Crear proyecto y módulos.

Procedimiento a seguir:

1. Inicie el software de configuración Security Configuration Tool en PC2.

2. Cree un nuevo proyecto con el siguiente comando de menú:

   Project ▸ New

   Se le pide que introduzca un nombre de usuario y una contraseña. Al usuario que usted introduce aquí se le asigna automáticamente la función de administrador.

3. Introduzca un nombre de usuario y una contraseña y confirme la entrada; con esto se crea un nuevo proyecto.

   Aparece automáticamente el diálogo "Seleccionar un módulo o configuración de software".

4. Configure ahora el tipo de producto "SOFTNET Configuration (SOFTNET Security Client, MD74x)", el módulo "SOFTNET Security Client", la versión de firmware "V3.0" y asígnele el nombre de módulo "SSC-PC2".

5. Cierre el cuadro de diálogo con "OK".

6. Cree un 2º módulo con el siguiente comando de menú:

   Insert ▸ Module

   Configure ahora el tipo de producto "SOFTNET Configuration (SOFTNET Security Client, MD74x)", el módulo "MD74x" y asígnele el nombre de módulo "MD741-1".

7. Haga clic ahora en el área "Configuración" dentro del campo "IP Address (ext.)" e introduzca ésta en el formato predeterminado. Configure además la máscara de subred externa correspondiente.

   Nota

   Para la configuración de este ejemplo es obligatoriamente necesario disponer de una dirección IP pública, no-modificable, para la tarjeta SIM del MD 741-1 del propio proveedor (de telefonía móvil), a la que no se pueda acceder a través de internet. Introduzca la dirección IP como dirección IP externa para su módulo.

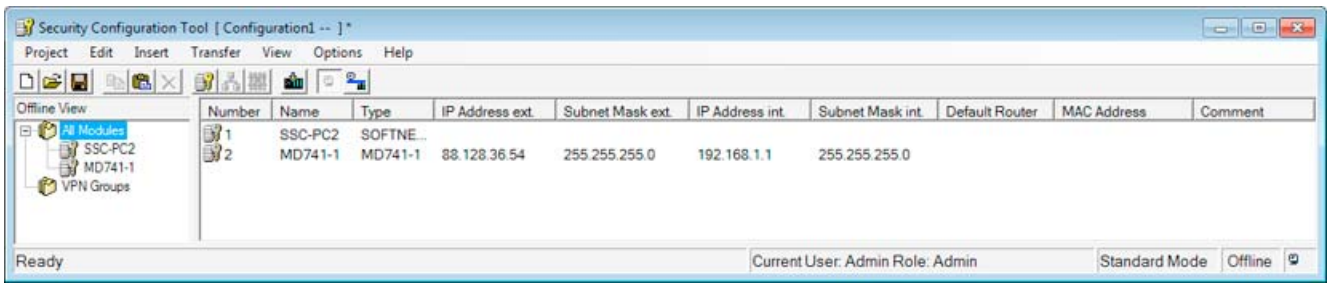
   Si trabaja con direcciones dinámicas para el MD741-1, necesitará una dirección DynDNS para el módulo. En este caso no necesita adaptar la dirección IP externa en este lugar. La dirección IP insertada sirve únicamente como comodín.

   En la configuración del SOFTNET Security Client, indique posteriormente un nombre DNS en lugar de una dirección IP externa.

8. Haga clic ahora en la zona "Configuración" dentro del campo "IP Address (int.)" e introduzca ésta en el formato predeterminado. (Dirección IP: 192.168.1.1). Configure además la máscara de subred interna correspondiente. (Máscara de subred: 255.255.255.0)

9. Cierre ahora el cuadro de diálogo con "OK".

Obtendrá ahora una vista correspondiente a la siguiente figura.


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
SSC-PC2
MD741-1
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 SSC-PC2 SOFTNE...
2 MD741-1 MD741-1 88.128.36.54 255.255.255.0 192.168.1.1 255.255.255.0
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

3.5.5 Configurar la conexión de túnel

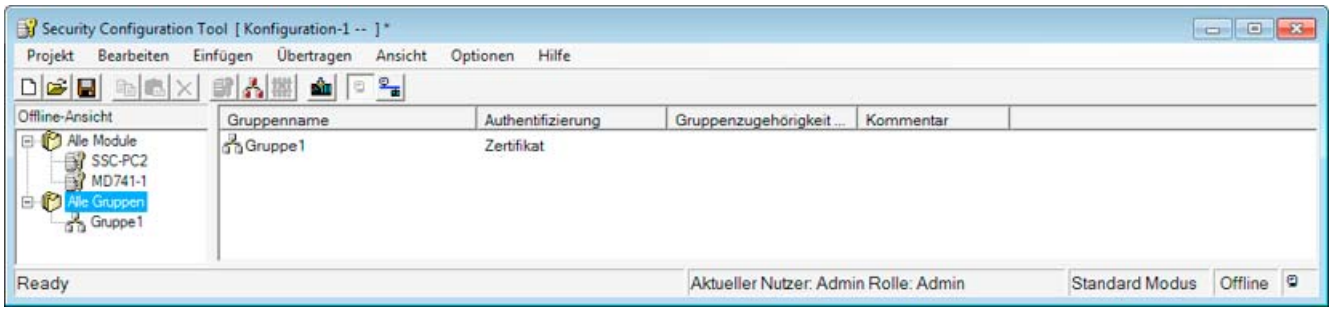
Un MD741-1 y el SOFTNET Security Client pueden crear exactamente un túnel IPSec para la comunicación segura si están asignados a un mismo grupo en el proyecto.

Procedimiento a seguir:

1. Seleccione en el área de navegación "All Groups" y cree un nuevo grupo con el siguiente comando de menú:

   Insert ▸ Group

   Este grupo recibe automáticamente el nombre "Group 1".



2. Seleccione en el área de contenido el módulo de MD741-1 "MD741-1" y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora a ese grupo o bien es miembro de ese grupo.

   El color del símbolo de llave del icono de módulo cambia ahora de gris a azul. Lo que expresa es que para el módulo, se ha configurado una conexión IPsec.

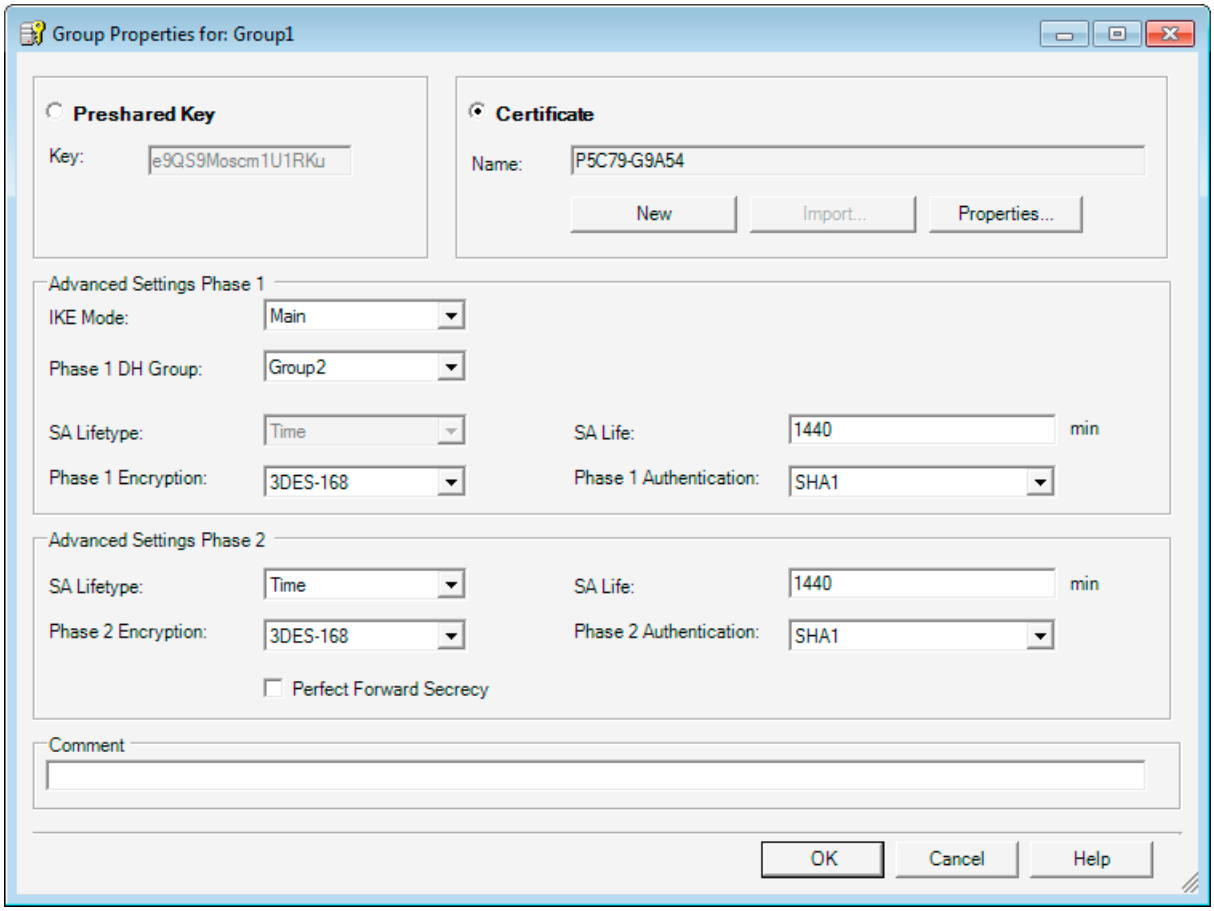
3. Seleccione en el área de contenido el módulo SOFTNET Security Client "SSC-PC2" y arrástrelo a "Group 1" en el área de navegación.

   El módulo está asignado ahora también a ese grupo.

4. Traslade ahora su proyecto al "Modo ampliado", en el que encontrará el siguiente comando de menú:

   View ▸ Advanced Mode

5. Abra las propiedades de grupo del Grupo 1 seleccionado en el menú de contexto "Propiedades..".
6. Modifique la duración SA de la fase 1 y de la fase 2 en 1440 minutos y deje todos los demás ajustes en sus valores por defecto.



ATENCIÓN

Sólo se puede crear una conexión de túnel correcta entre MD741-1 y SOFTNET Security Client si respecta estrictamente los siguientes parámetros.

El uso de parámetros diferentes puede ocasionar que los dos partner de tunneling no puedan establecer entre sí conexión VPN alguna.

Procedimiento de autenticación: Certificado

Advanced Settings Phase 1:

- IKE Mode: Main
- Phase 1 DH Group: Group2
- Phase 1 Encryption: 3DES-168
- Duración SA (minutos): 1440
- Phase 1 Authentication: SHA1

Advanced Settings Phase 2:

- SA Lifetype: Time
- Phase 2 Encryption: 3DES-168
- Duración SA (minutos): 1440
- Phase 2 Authentication: SHA1

7. Guarde ahora este proyecto con el siguiente comando de menú, bajo un nombre apropiado:

   Project ▸ Save As…

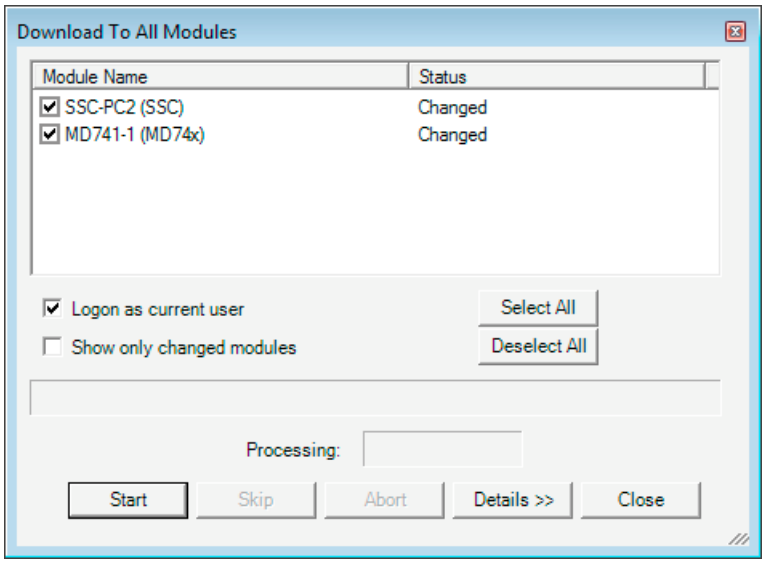
Con esto ha terminado la configuración de la conexión de túnel.

3.5.6 Guardar la configuración del MD741-1 y del SOFTNET Security Client

Procedimiento a seguir:

1. Llame el siguiente cuadro de diálogo con el comando aquí indicado:

Transfer ▸ To All Modules…



2. Inicie el proceso de carga con el botón "Start".
3. Guarde el archivo de configuración "Nombredeproyecto.sscPC2.dat" en su directorio del proyecto y asigne una contraseña como clave privada del certificado. En el directorio del proyecto se guardan los siguientes archivos:
   - "Projektname.SSC-PC2.dat"
   - "Nombredeproyecto.Seriedeletras.SSC-PC2.p12"
   - "Nombredelproyecto.Grupo1.cer"
4. Guarde el archivo de configuración "Nombredeproyecto.MD741-1.txt" en su directorio del proyecto y asigne una contraseña como clave privada del certificado. En su directorio del proyecto se guardan los siguientes archivos:
   - "Projektname.MD741-1.txt"
   - "Nombredeproyecto.Seriedeletras.MD741-1.p12"
   - "Nombredeproyecto.Grupo1.MD741-1.cer"

Ha guardado ahora todos los archivos y certificados necesarios y puede poner en servicio el MD741-1 y el SOFTNET Security Client.

3.5.7 Realizar la configuración del MD741-1

Con la ayuda del archivo de texto guardado "Nombredelproyecto.MD741-1.txt", puede llevar a cabo fácilmente la configuración con la Web Based Management del MD741-1. A continuación, tomando este ejemplo, se le muestra paso a paso la configuración del MD741-1.

Para la configuración se realiza lo siguiente:

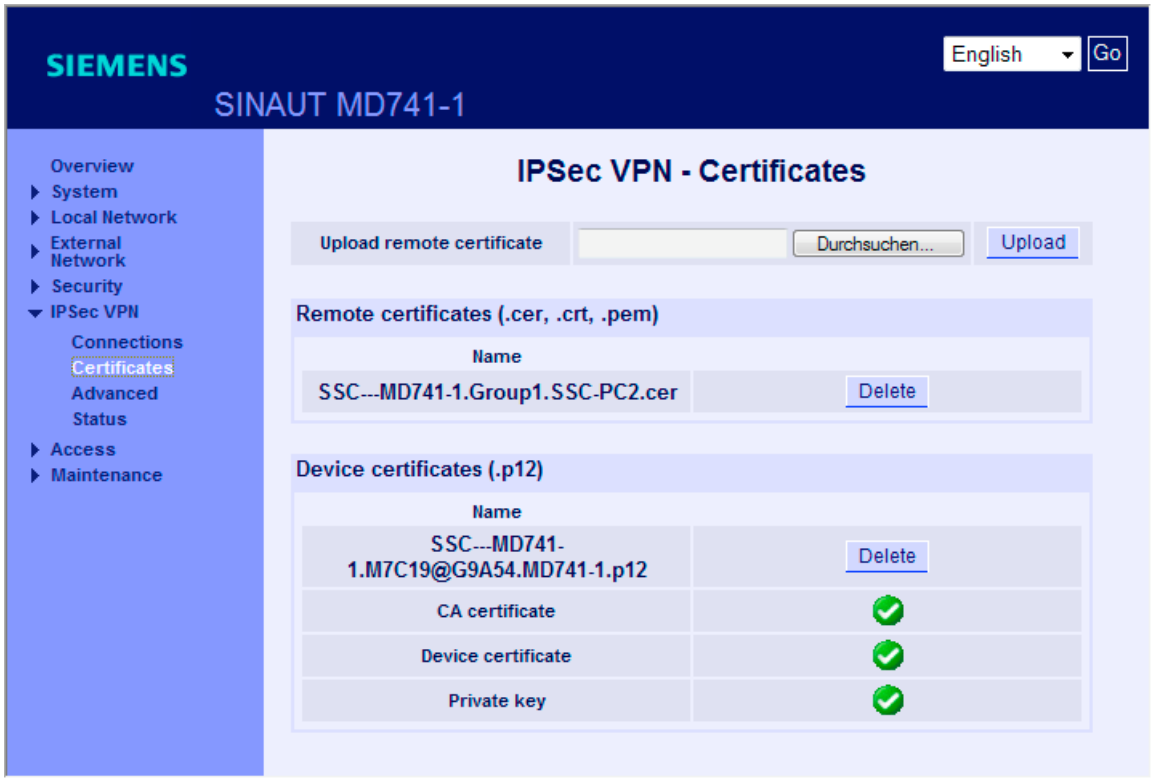
- el MD741-1 recibe una dirección IP pública fija a la que se puede acceder vía internet;
- el SOFTNET Security Client recibe una dirección IP dinámica del proveedor.

Paralelamente se le indicará donde corresponda que configure un nombre DynDNS para el MD741-1.

Procedimiento a seguir:

1. Conéctese por medio del PC1 con la plataforma web del MD741-1.
   Observación: Si el MD741-1 tiene ajustes de fábrica, entonces la interfaz interna del módulo tiene la dirección IP 192.168.1.1
2. Navegue por el siguiente directorio:

   IPSec VPN ► Certificados
3. Ha guardado los certificados necesarios en el último capítulo de PC2, y ha indicado una contraseña para la clave privada. Transfiera primero los certificados ("Nombredelproyecto.Seriedeletras.MD741-1.p12", "Nombredelproyecto.Grupo1.MD741-1.cer") para el MD741-1 al PC1.
4. Cargue ahora los interlocutores del certificado "Nombredeporyecto.Grupo1.MD741-1.cer", y el archivo PKCS 12 "Nombredelproyecto.Seriedeletras.MD741-1.p12", en el módulo.



Modo VPN Roadwarrior del MD741-1

Puesto que el SOFTNET Security Client dispone de una dirección IP dinámica, se utiliza el modo VPN Roadwarrior del MD741-1 para establecer una conexión segura.

- Modo Roadwarrior del MD741-1:
  - En el modo VPN Roadwarrier, el SINAUT MD741-1 puede aceptar conexiones VPN de interlocutores con dirección desconocida. Se pueden aplicar de forma móvil, por ejemplo, interlocutores que obtengan de forma dinámica su dirección de IP.
  - La conexión VPN debe ser establecida a través de los interlocutores. Es posible una conexiión VPN en el modo Roadwarrior. Las conexiones VPN en el modo estándar pueden, para ello, ser operadas en paralelo.

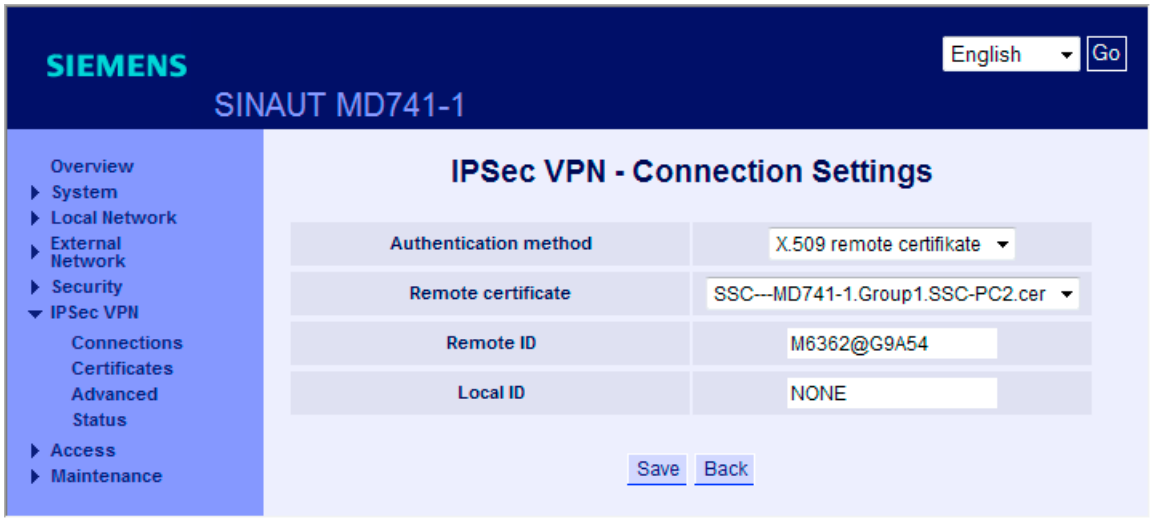
Procedimiento a seguir:

1. Navegue por el siguiente directorio:

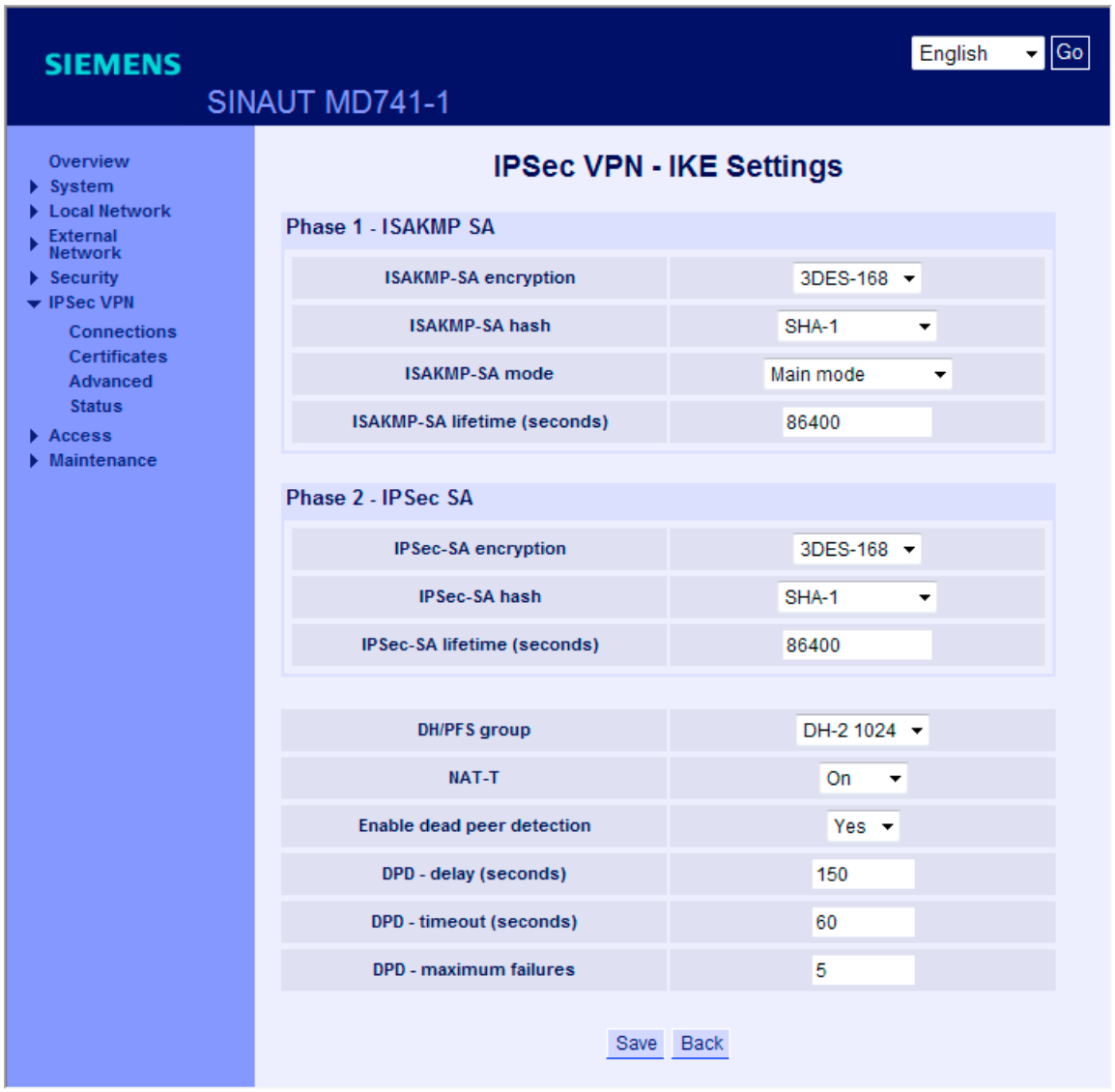
   IPSec VPN ► Conexiones

2. Realice los ajustes del Roadwarrior VPN tal y como se muestra en la siguiente figura, y guárdelos.

   Puede determinar el "Remote ID" desde su archivo de texto "Nombredelproyecto.MD741-1.txt". La entrada del "Remote ID" es posible opcionalmente.



3. Realice los ajustes IKE del Roadwarrior VPN tal y como se muestra en el siguiente gráfico, y guárdelos.



ATENCIÓN

Sólo se puede crear una conexión de túnel correcta entre MD741-1 y SOFTNET Security Client si se respectan estrictamente los siguientes parámetros.

El uso de parámetros diferentes hace que los dos partner de tunneling no establezcan entre sí conexión VPN alguna. Aténgase por favor siempre a los ajustes indicados en el archivo de texto recibido (como se indica a continuación)

Procedimiento de autenticación:X.509 certificado de interlocutores

Fase 1 - ISKAMP SA:

- ISAKMP-SA encriptación:3DES-168
- ISAKMP-SA Hash: SHA-1
- Modo ISAKMP-SA: Main Mode
- ISAKMP-SA vida (segundos): 86400

Fase 2 - IPSec SA:

- Encriptación IPSec SA: 3DES-168
- IPSec SA Hash: SHA-1
- PSec SA vida (segundos): 86400

Grupo DH/PFS: DH-2 1024

4. Para poder utilizar la función de diagnóstico del SOFTNET Security Client para un túnel VPN correctamente establecido en conexión con el MD741-1, deberá admitir un Ping de la red externa del MD741-1.

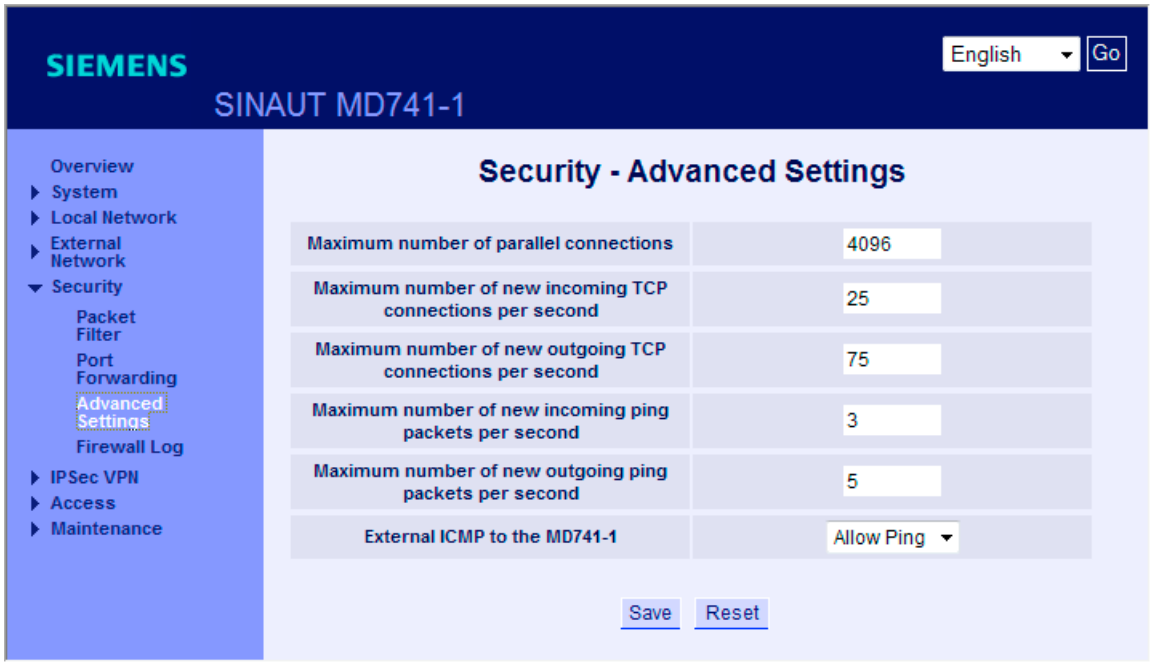
   Navege para ello por el directorio:

   Security ▸ Advanced

   Ponga la función "ICMP de externa a MD741-1" en el valor "Permitir ping", y guarde el cambio. Para ello deberá observar lo que se expresa en el siguiente gráfico.

   Nota

   Si no autoriza esta función, entonces no puede utilizar la función de diagnóstico del SOFTNET Security Client para un túnel VPN corectamente construido en conexión con el MD741-1. Entonces no recibirá mensaje alguno sobre si el túnel se ha establecido correctamente, pero puede comunicarse de forma segura a través del túnel.



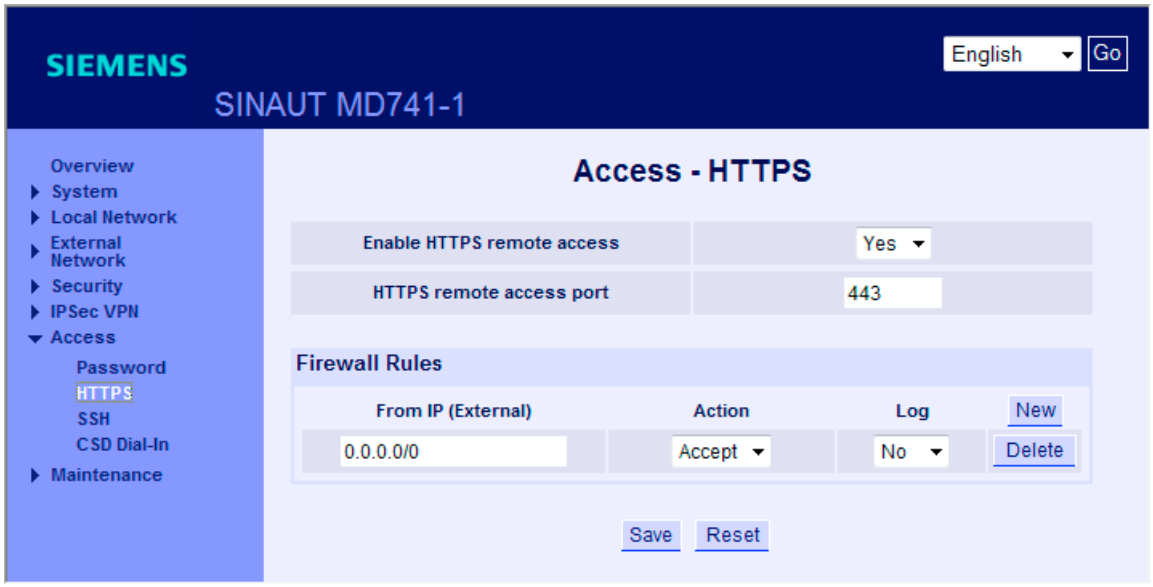
5. Para poder llegar a la interfaz web del módulo MD741-1 también a través de la interfaz externa, autorice el acceso remoto HTTPS.

   De esta forma tiene la posibilidad de configurar y de diagnosticar a distancia el MD741-1 a través de un túnel.

   Navege para ello por el directorio:

   Acceso▸ HTTPS

   Ponga la función "Activar el acceso remoto HTTPS" en el valor "Sí", como se muestra en el siguiente gráfico, y guarde los cambios.

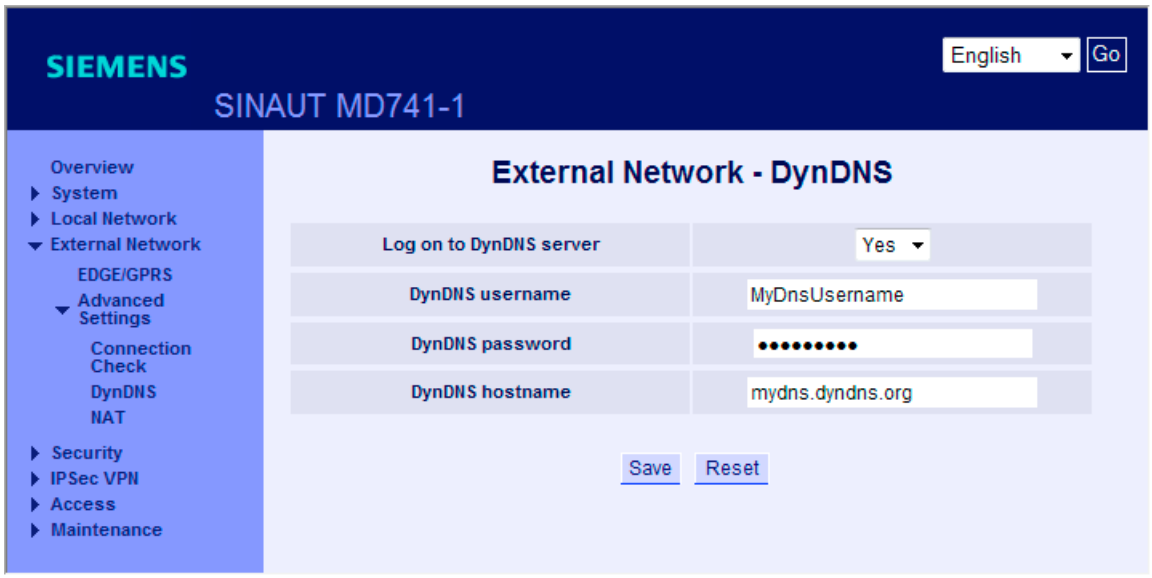


Nota

Si desea llegar al MD741-1 por medio de un nombre DNS, parametrice en el siguiente directorio la conexión del DynDNS Server:

External Network ► Advanced Settings ►DynDNS

1. Cambie el ajuste "Notificar este MD741 en un DynDNS Server" al valor "Sí".
2. Indique su nombre de usuario y la contraseña de su DynDNS Account.
3. Introduzca íntegramente la dirección DynDNS en el campo "DynDNS Hostname". Cuídese de indicar también el dominio de esta dirección. (Ej.: "mydns.dyndns.org")



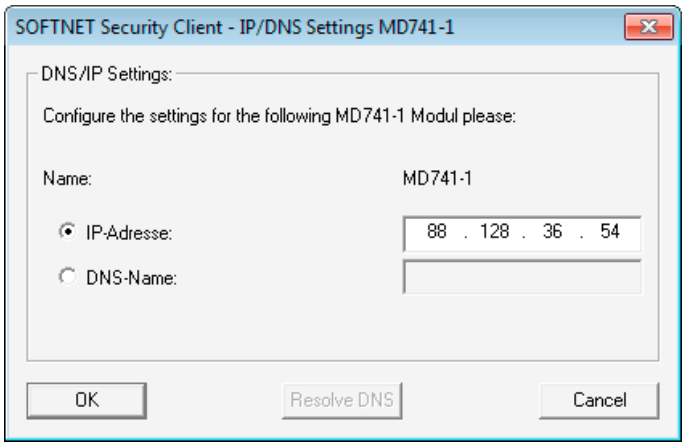
De esta forma se concluye la puesta en servicio del módulo MD741-1. El módulo y el SOFTNET Security Client pueden constituir un túnel de comunicación a través del cual pueden comunicarse de forma segura los nodos de red de la red interna con PC2.

3.5.8 Construcción del túnel con el SOFTNET Security Client

Procedimiento a seguir:

1. Inicie el SOFTNET Security Client en PC2.
2. Pulse el botón "Load Configuration", cambie a su directorio del proyecto y cargue el archivo de configuración "Nombredeproyecto.SSC-PC2.dat".
3. Para una configuración MD741-1, el SOFTNET Security Client abre el diálogo "Ajustes IP/DNS MD741-1". En este diálogo, indique la dirección IP pública del módulo MD741-1 que haya recibido de su proveedor. Confirme el cuadro de diálogo con "OK".

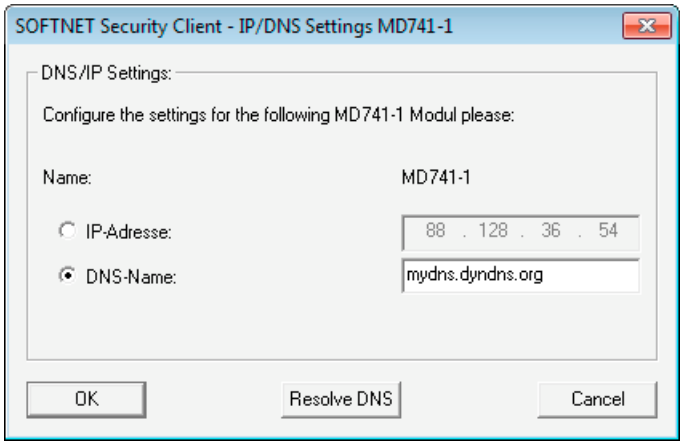
   Observación: Si trabaja con un nombre DNS, entonces puede configurarlo en dicho cuadro de diálogo en lugar de una dirección IP.



4. Introduzca la contraseña para el certificado y confirme con "Next".
5. Confirme el diálogo "Activate static configured members?" con "Yes".
6. Accione el botón "Tunnel Overview"

Nota

Si desea llegar al módulo MD741-1 a través de un nombre DNS, en el paso 3 puede parametrizar la dirección DynDNS íntegra en el campo de entrada "Nombre DNS". (Ej.: "mydns.dyndns.org")



Resultado: conexión de túnel activa

Se ha establecido el túnel entre MD741-1 y SOFTNET Security Client.

Tomando el icono azul en la entrada "MD741-1" está usted reconociendo que se ha establecido una Policy para esta conexión de comunicación.

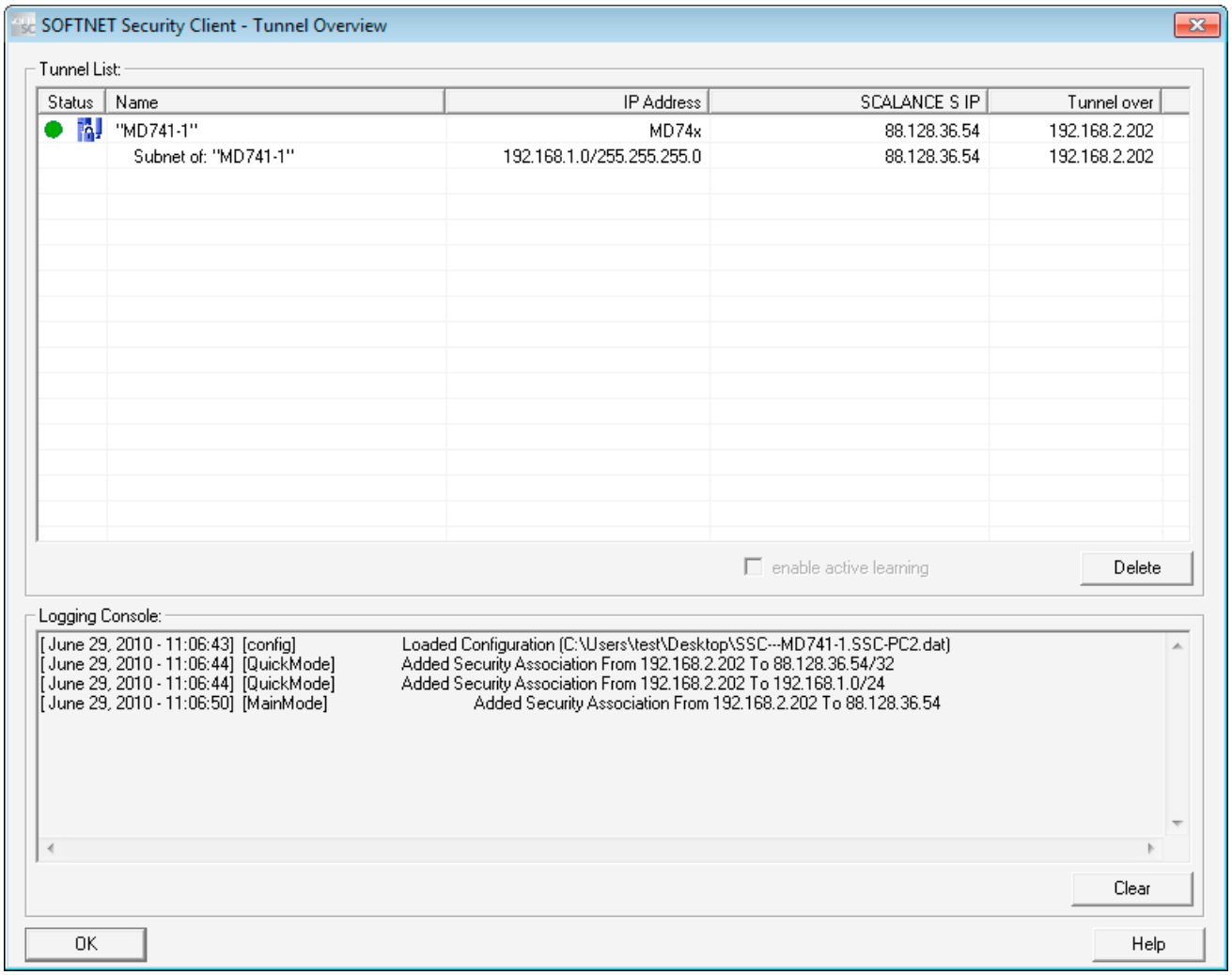
El estado operativo de que se puede alcanzar el MD741-1,se señala mediante el "círculo verde" al introducir "MD741-1".

Nota

Tenga en cuenta que esta función es independiente de la autorización de la función ping en el módulo MD741-1.

En la consola Log de la vista de túnel del SOFTNET Security Client recibirá adicionalmente algunos mensajes de su sistema entre los que podrá usted elegir:

- ¿Cómo se desarrolla el intento de conexión?
- ¿Se ha establecido la Policy para la conexión de comunicación?



Con esto ha terminado la puesta en servicio de la configuración. El módulo MD741-1 y el SOFTNET Security Client han constituidor un túnel de comunicación a través del cual pueden comunicarse de forma segura los nodos de red de la red interna con PC2.

3.5.9 Probar la función del túnel (prueba Ping)

¿Cómo se puede probar la función configurada?

La prueba de la función se realiza con un comando "ping" tal como se describe a continuación.

Como alternativa se pueden utilizar otros programas de comunicación para el test de la configuración.

ATENCIÓN
En caso de Windows, el cortafuegos (Firewall) puede estar ajustado como estándar de manera que no puedan pasar comandos Ping. Eventualmente tendrá que habilitar los servicios ICMP del tipo Request y Response.

Sección de la prueba

Compruebe ahora el funcionamiento de la conexión de túnel establecida entre PC1 y PC2 del siguiente modo:

1. En el PC2, llame en la barra de inicio el siguiente comando de menú:

   Inicio ▸ Programas ▸ Accesorios ▸ Símbolo del sistema

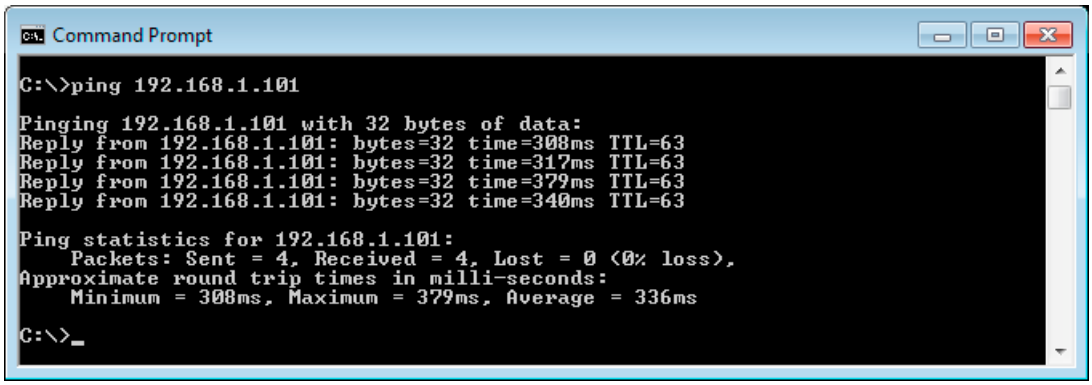
2. Entrada del comando Ping de PC2 a PC1 (dirección IP 192.168.1.101).

   Directamente en la línea de comandos de la ventana presentada "Símbolo del sistema", introduzca en la posición del cursor el comando

   Ping 192.168.1.101

   .

Aparecerá entonces el siguiente mensaje: (respuesta positiva del PC1).


Command Prompt
C:\>ping 192.168.1.101
Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=308ms TTL=63
Reply from 192.168.1.101: bytes=32 time=317ms TTL=63
Reply from 192.168.1.101: bytes=32 time=379ms TTL=63
Reply from 192.168.1.101: bytes=32 time=340ms TTL=63
Ping statistics for 192.168.1.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 308ms, Maximum = 379ms, Average = 336ms
C:\>

Resultado

Cuando los telegramas IP llegan al PC1, la "estadística Ping" muestra para 192.168.1.101 lo siguiente:

- Enviado = 4
- Recibido = 4
- Perdido = 0 (0 % pérdida)

Dado que no estaba permitida ninguna otra comunicación, esto telegramas sólo se pueden haber transportado por el túnel VPN.

Configuración con Security Configuration Tool 4

Security Configuration Tool es la herramienta de configuración suministrada junto con el SCALANCE S.

El presente capítulo le familiariza con la interfaz de operación y el funcionamiento de la herramienta de configuración.

En él se describen la instalación, el manejo y la administración de proyectos SCALANCE S.

Otras informaciones

En los capítulos sucesivos de este manual se explica con detalle la configuración de módulos y de túneles IPsec.

La ayuda online le proporcionará también información detallada sobre los diálogos y los parámetros ajustables. Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

4.1 Funciones y funcionamiento

Prestaciones

La herramienta de configuración Security Configuration Tool se utiliza para las siguientes tareas:

- Configuración de SCALANCE S
- Configuración de SOFTNET Security Client (S612 / S613 / MD 741-1)
- Creación de datos de configuración para MD 740-1 / MD 741-1
- Funciones de test y diagnóstico, indicaciones de estado

Modos de funcionamiento

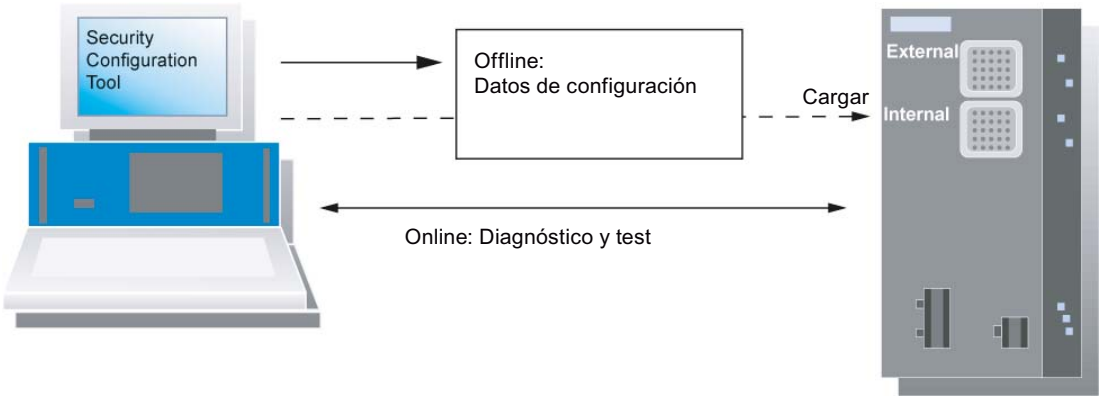
La Security Configuration Tool puede trabajar de dos modos:

- Offline - Vista de configuración

  En el modo offline se ajustan los datos de configuración para los módulos SCALANCE S y SOFTNET Security Client. Antes de la carga se tiene que haber establecido para esto una conexión con un SCALANCE S.

- Online

  El modo online sirve para comprobar y diagnosticar un SCALANCE S.



Dos vistas de operación

En el modo offline, la Security Configuration Tool proporciona dos vistas de operación:

- Standard Mode

  El Standard Mode está preajustado en la Security Configuration Tool. Permite una configuración rápida y sin complicaciones para el uso de SCALANCE S.

- Advanced Mode

  En el Advanced Mode existen otras posibilidades de ajuste que permiten ajustar de forma personalizada las reglas de firewall y las funciones de seguridad.

Forma de trabajar - Seguridad y coherencia

- Sólo pueden acceder usuarios autorizados

  Cada proyecto se puede proteger de acceso no autorizado asignando contraseñas.

- Datos de proyecto coherentes

  Ya durante la entrada en los distintos cuadros de diálogo se realizan comprobaciones de la coherencia. Además puede iniciar en todo momento una prueba de coherencia a nivel de proyecto, en la que se incluyen todos los cuadros de diálogo.

  Sólo se pueden cargar datos de proyecto coherentes.

- Protección de datos de proyecto por codificación

  Los datos de proyecto y configuración almacenados están protegidos por codificación tanto en el archivo de proyecto como en el C-Plug.

4.2 Instalación

La herramienta de configuración Security Configuration Tool se instala desde el CD SCALANCE S adjuntado.

Requisitos

Los siguientes requisitos se han de cumplir para la instalación y el uso de la Security Configuration Tool en un PC/PG:

- Sistema operativo Windows XP SP2 o SP3 (no Home), Windows 7 (no Home);
- PC/PG con al menos 128 MByte de memoria RAM y una CPU con una frecuencia de reloj de al menos 1 GHz.

Procedimiento a seguir

ATENCIÓN
Antes de proceder a la instalación de la Security Configuration Tool, lea el archivo "README" del CD adjuntado. En este archivo encontrará informaciones importantes así como referencias a las últimas modificaciones.

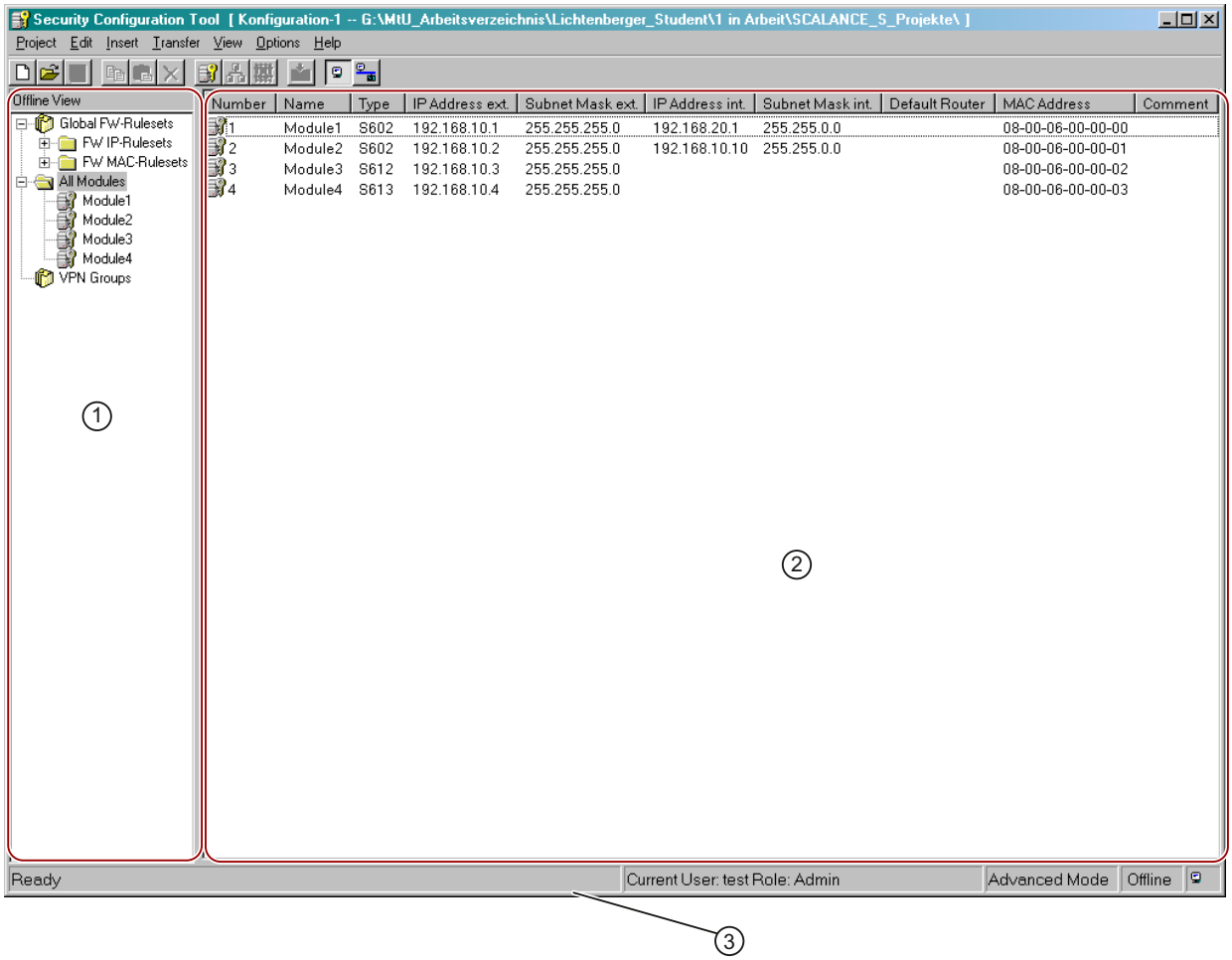
- Introduzca el CD SCALANCE S en la unidad CD-ROM; si está conectada la función Autorun, se inicia automáticamente la superficie de operación desde a que puede realizar la instalación.

o

- Inicie la aplicación "start.exe" existente en el CD SCALANCE S.

4.3 Interfaz de usuario y comandos de menú

Estructura de la interfaz de usuario



① El ámbito de navegación funciona como explorador del proyecto con las siguientes carpetas principales:

- Reglas globales de Firewall

  El nodo contiene el juego de reglas de firewall global proyectado. Otras carpetas se distinguen en:
  - Juego de reglas de IP
  - Juego de reglas MAC
- Todos los módulos

  El nodo contiene los módulos proyectados SCALANCE S o SOFTNET Security Clients del proyecto.
- Todos los grupos

  El nodo "Todos los grupos" contiene todos los VPNs producidos.

Si selecciona un objeto en el área de navegación obtendrá en el área de contenido informaciones detalladas sobre ese objeto.

② Índice:

Si selecciona un objeto en el área de navegación obtendrá en el área de contenido informaciones detalladas sobre ese objeto.

Se pueden introducir los parámetros uno a uno.

Haciendo doble clic en los objetos se abren los cuadros de diálogo de propiedades para introducir los demás parámetros.

③ Barra de estado

La línea de estado puesta los estados operativos y los mensajes de estado actuales; a éstos pertenecen:

- Los usuarios actuales y el tipo de usuario
- La vista de operación - Standard Mode / Advanced Mode
- El tipo de operación - Online / Offline

Barra de menús

A continuación se ofrece un cuadro general de los comandos de menú seleccionables y su significado.

Comando de menú		Significado / observaciones	Shortcut
Project ▸…		Funciones para ajustes específicos del proyecto, así como la carga y el almacenamiento del archivo del proyecto.	
	New	Crear nuevo proyecto	
	Open...	Abrir un proyecto ya existente.	
	Save	Guardar un proyecto abierto en la ruta y con el nombre de proyecto actuales.	
	Save As...	Guardar un proyecto abierto en una ruta y con un nombre de proyecto seleccionables.	
	Properties...	Abrir un cuadro de diálogo para propiedades del proyecto.	
	Recent Projects	Posibilidad de seleccionar directamente los proyectos procesados hasta el momento	
	Quit		
Edit ▸…		Nota: A las funciones aquí mencionadas se puede accedeer también en parte, para el objeto seleccionado, a través del menú desplegable con el botón derecho del ratón.	
	Copy	Copiar el objeto seleccionado.	Ctrl+C
	Paste	Traer el objeto del portapapeles e insertarlo ("pegarlo").	Ctrl+V
	Del	Borrar el objeto seleccionado.	Borr.
	Rename	Cambiar de nombre el objeto seleccionado.	F2
	Properties	Abrir el diálogo de propiedades del objeto seleccionado.	F4
	Online Diagnostics…	Acceder a las funciones de test y diagnóstico. Este comando sólo está visible en la vista Online.	
Insert ▸…		(comandos de menú disponibles sólo en el modo offline)	

Comando de menú		Significado / observaciones	Shortcut
	Module	Crear nuevo módulo. Este comando sólo está activo si está seleccionado un objeto Module o Group en el área de navegación.	Ctrl+M
	Group	Crear nuevo grupo. Este comando sólo está activo si está seleccionado un objeto Grupos en el área de navegación.	Ctrl+G
	Firewall rule set	Crear un nuevo bloque de reglas IP o MAC de validez global para el firewall. Este comando sólo está activo si está seleccionado un objeto Firewall en el área de navegación.	Ctrl+F
Transfer ▸…			
	To Module...	Cargar datos en los módulos seleccionados. Observación: Sólo se pueden cargar datos de proyecto coherentes.	
	To All Modules...	Cargar datos en todos los módulos configurados. Observación: Sólo se pueden cargar datos de proyecto coherentes.	
	Configuration Status…	Mostrar en una lista los estados de configuración de los módulos configurados.	
	Firmware Update...	Cargar nuevo firmware en el SCALANCE S seleccionado.	
View ▸…			
	Advanced Mode	Cambiar del Standard Mode al Advanced Mode. Atención: Una conmutación realizada al Advanced Mode para el proyecto actual sólo se puede anular mientras no se hayan efectuado modificaciones. Está preajustado el Standard Mode.	Ctrl+E
	Offline	Es preajuste.	Ctrl+Shift+D
	Online		Ctrl+D
Options ▸…			
	IP Service Definitions...	Abrir cuadro de diálogo para definiciones de los servicios para las reglas IP Firewall. Este comando sólo está visible en la vista "Advanced Mode".	
	MAC Service Definitions…	Abrir cuadro de diálogo para definiciones de los servicios para las reglas MAC Firewall. Este comando sólo está visible en la vista "Advanced Mode".	
	Project Change Password…	Función para cambiar la contraseña de usuario.	
	Network Adapters…	Función para seleccionar el adaptador de red local a través del que se debe establecer una conexión con el SCALANCE S.	
	Log Files...	Visualización de archivos Log. Se pueden leer archivos Log y se pueden iniciar registros en Log.	
	Symbolic Names...	Asignación de nombres simbólicos para direcciones IP o MAC.	

Comando de menú		Significado / observaciones	Shortcut
	Pruebas de coherencia ("Check Consistency")	Comprobación de la coherencia de todo el proyecto. Se presenta una lista de resultados.	
Help ▸…			
	Contenido...	Ayuda para las funciones y los parámetros que encontrará en la Security Configuration Tool.	Ctrl+Shift+F1
	Índice alfabético...	Ayuda para las funciones y los parámetros que encontrará en la Security Configuration Tool.	Ctrl+Shift+F2
	Info…	Información sobre la versión de la Security Configuration Tool.	

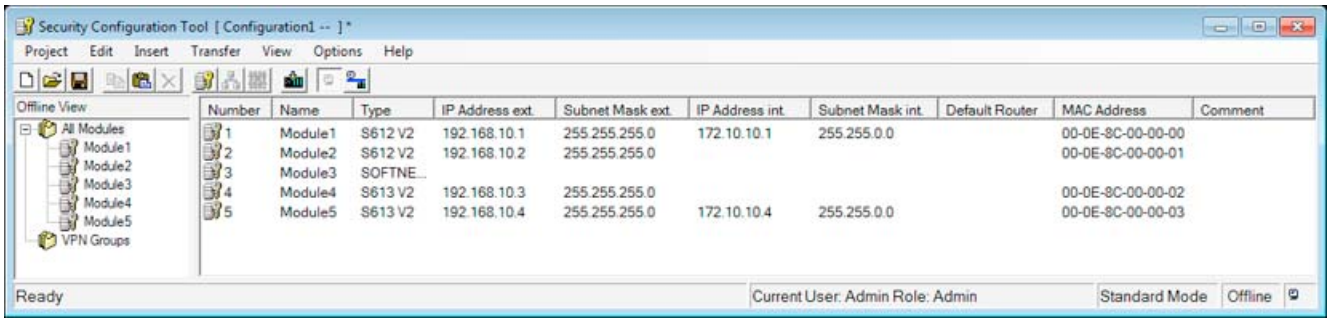
4.4 Administración de proyectos

4.4.1 Resumen

Proyecto SCALANCE S

En la Security Configuration Tool, un proyecto abarca todas las informaciones de configuración y administración para uno o varios equipos SCALANCE S, SOFTNET Security Client y MD74x.

Para cada equipo SCALANCE S, cada SOFTNET Security Client y cada MD74x se crea un módulo en el proyecto.


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
VPN Groups
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 172.10.10.1 255.255.0.0 00-0E-8C-00-00-00
2 Module2 S612 V2 192.168.10.2 255.255.255.0 00-0E-8C-00-00-01
3 Module3 SOFTNE...
4 Module4 S613 V2 192.168.10.3 255.255.255.0 00-0E-8C-00-00-02
5 Module5 S613 V2 192.168.10.4 255.255.255.0 172.10.10.4 255.255.0.0 00-0E-8C-00-00-03
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

En general, las configuraciones de un proyecto contienen:

- Ajustes válidos para todo el proyecto
- Ajustes específicos de los módulos
- Asignaciones a grupos para túnel IPsec (S612 / S613 / SOFTNET Security Client)

Además, una administración de usuarios regula los derechos de acceso a los datos del proyecto y con ello a los equipos SCALANCE S.

Ajustes válidos para todo el proyecto

- Propiedades del proyecto

  Éstas comprenden además de informaciones generales sobre direcciones y nombres, predeterminaciones para valores de inicialización y ajustes para autenticación.

- Bloques de reglas globales de Firewall

  Las reglas globales para firewall se pueden asignar a varios módulos a un tiempo. Esta posibilidad simplifica en muchos casos la configuración, a diferencia de la configuración de bloques de reglas locales para firewall en el caso de ajustes específicos de los módulos.

- Definiciones de servicios

  Con ayuda de definiciones de servicios IP se pueden definir reglas de firewall de forma compacta y clara.

Ajustes específicos de los módulos

La mayoría de las funciones se configuran en el cuadro de diálogo de propiedades de un módulo. Aquí se presenta una visión de conjunto de las fichas ofecidas y sus funciones:

Función / ficha en el diálogo de propiedades	se ofrece en el modo …	
	Standard	Advanced
Network Aquí puede indicar, si procede, direcciones de los router existentes en su red.	X	X
Firewall Aquí se activa en el Standard Mode el firewall con reglas estándar sencillas. Además puede activar aquí ajustes para Logging. En el Advanced Mode puede definir reglas detalladas para filtros de paquetes. También puede definir ajustes de Logging explícitos para cada regla de filtro de paquetes.	X	X
SSL Certificate Si es necesario, por ejemplo en caso de un certificado comprometido, puede importar un certificado o puede hacer que Security Configuration Tool cree un ceretificado nuevo.		X
Time Synchronization Defina aquí el tipo de sincronización para fecha y hora.	X	X
Logging Aquí puede definir parámetros más exactos para el modo de registro y memorización de eventos de Logging.		X

Función / ficha en el diálogo de propiedades	se ofrece en el modo …	
	Standard	Advanced
Nodos Para un módulo que esté en el modo Bridge se pueden configurar aquí las subredes internas estáticas así como los nodos IP/MAC intrnos y se puede permitir o bloquear el aprendizaje de nodos internos. Para un módulo que esté en el modo Routing, se pueden introducir participantes internos / subredes completas que se deben tunelar.		X
VPN Si el módulo se encuentra en un grupo, aquí se puede configurar la Dead-Peer-Detection, la forma de establecimiento de la conexión y la dirección IP para WAN.		X
Routing Modus Aquí se activa en el Standard Mode la función "Router". En el Advanced Mode se puede activar adicionalmente la función NAT/NAPT Router y se puede fijar en una lista la conversión de direcciones.	X	X
Servidor DHCP Puede activar, para la red interna, el módulo como DHCP Server.		X

Encontrará la descripción detallada de estas funciones en el capítulo "Firewall, Router y otras propiedades de los módulos".

Asignaciones a grupos para túnel IPsec (S612 / S613 / SOFTNET Security Client)

Con esto se fija qué módulos SCALANCE S, SOFTNET Security Clients y módulos MD74x pueden comunicarse entre sí a través de túnel IPsec.

Al asignar módulos SCALANCE S, SOFTNET Security Clients y módulos MD74x a un grupo, esos módulos pueden establecer un túnel de comunicación a través de una VPN (virtual private network).

Sólo módulos del mismo grupo se pueden comunicar entre sí de forma segura a través de túnel; los módulos SCALANCE S, los SOFTNET Security Clients y los módulos MD74x pueden pertenecer a varios grupos al mismo tiempo.

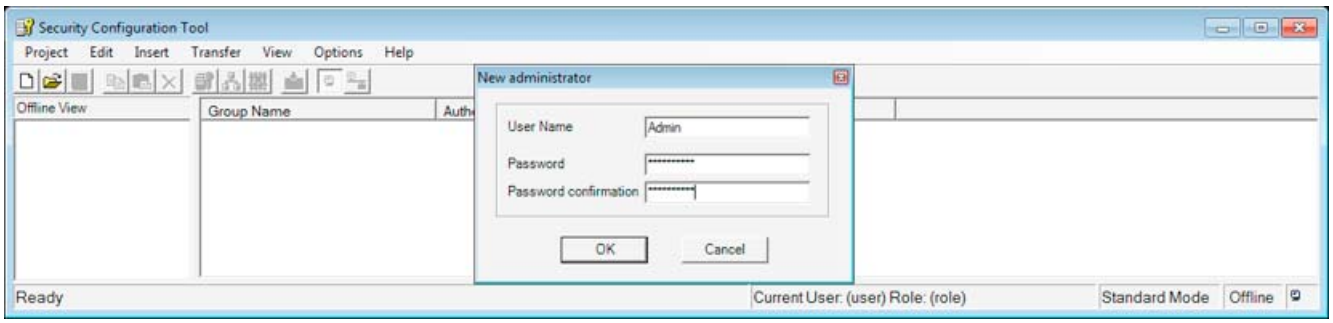
4.4.2 Creación y edición de proyectos

Creación de un proyecto

Seleccione el comando de menú:

Project ▸ New...

Se le pide que introduzca un nombre de usuario y una contraseña. El usuario aquí creado es del tipo Administrator.



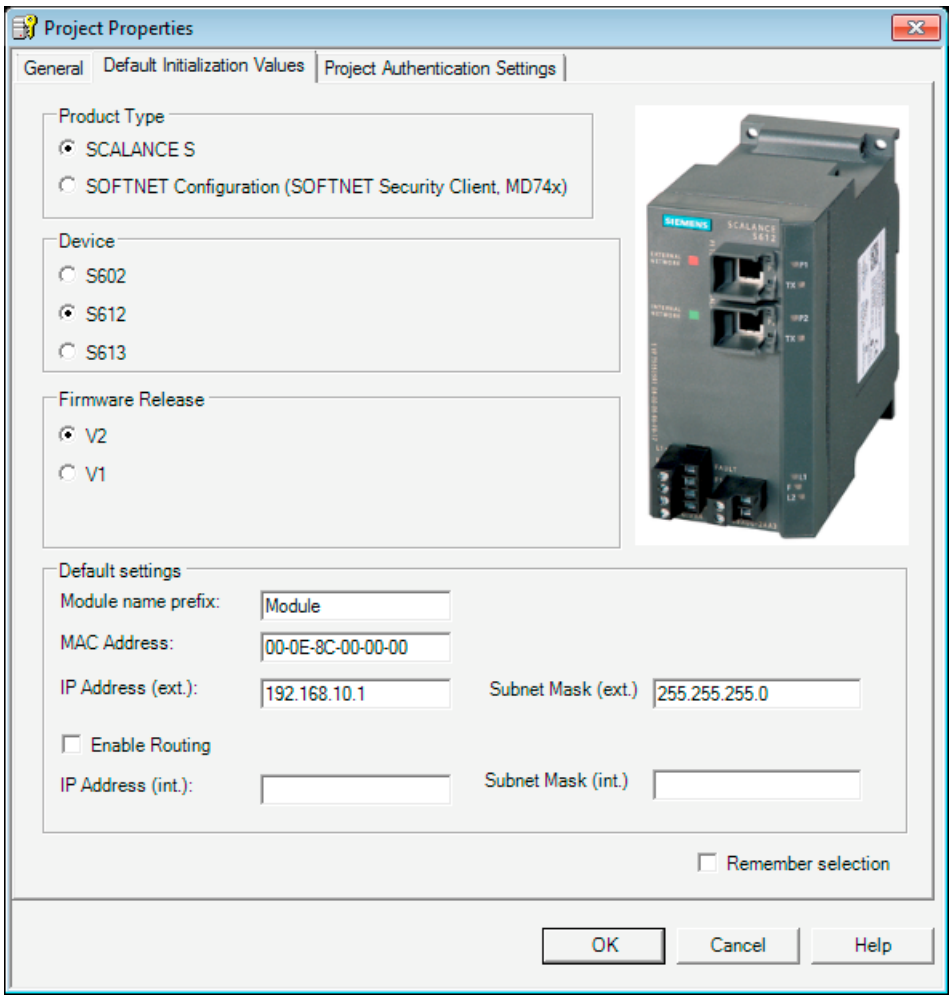
Security Configuration Tool crea un proyecto estándar y abre automáticamente el diálogo "Selección de un módulo o configuración de software", en el que puede usted configurar su primer módulo.

Definición de valores de inicialización para un proyecto

Con los valores de inicialización se definen propiedades que se adoptan automáticamente al crear nuevos módulos.

Seleccione el siguiente comando de menú para la entrada de valores de inicialización:

Project ▸ **Properties…**, ficha "Valores de incialización estándar".



Protección de datos de proyecto por codificación

Los datos de proyecto y configuración almacenados están protegidos por codificación tanto en el archivo de proyecto como en el C-Plug.

Consulte también

Firewall, Router y otras propiedades del módulo (Página 129)

4.4.3 Configuración de usuarios

Tipos de usuarios y derechos

El acceso a los proyectos y módulos SCALANCE S es administrado a través de configuraciones de usuarios. SCALANCE S conoce dos tipos de usuarios con diferentes derechos o autorizaciones:

- Administrators

  Con la categoría de usuario del tipo "Administrator" está autorizado a acceder sin limitaciones a todos los datos de configuración y a los módulos SCALANCE S.

- User

  Con la categoría de usuario del tipo "user" tiene las siguientes autorizaciones de acceso:

  – Acceso de lectura a configuraciones; excepción: se permite modificar la contraseña propia.

  – Acceso de lectura a SCALANCE S en el modo "Online" con fines de test y diagnóstico.

Autenticación del usuario

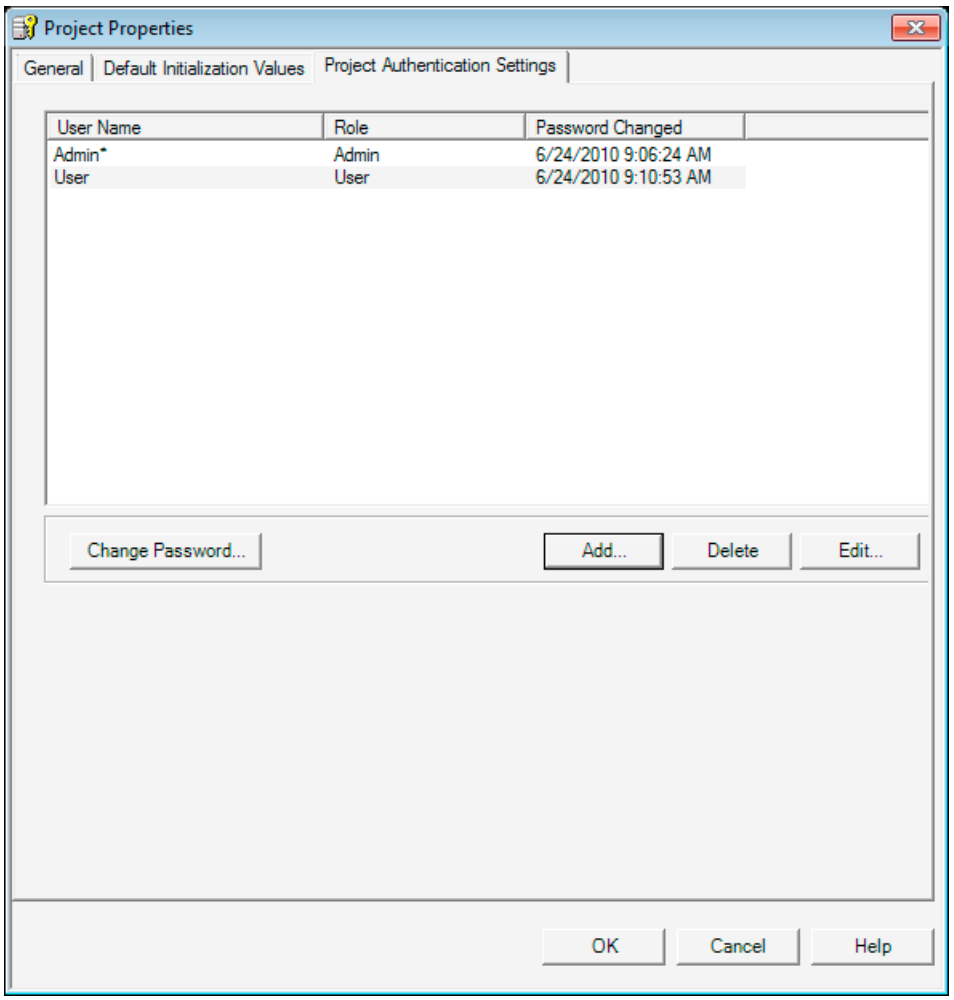
El usuario del proyecto se tiene que autenticar para el acceso. Para cada usuario se puede fijar una autenticación por contraseña.

ATENCIÓN
Debería guardar sus contraseñas de usuario en un lugar seguro. Si olvida sus contraseñas de usuario ya no podrá acceder al proyecto en cuestión ni a sus configuraciones ni a los módulos SCALANCE S. Entonces sólo podrá acceder a los módulos SCALANCE S con una "Reposición a la configuración de fábrica", con lo que se pierden las configuraciones.

Cuadro de diálogo para configurar usuarios

Seleccione el siguiente comando de menú para la configuración de usuarios:

Project ▸ Properties…, ficha "Authentication Settings".



Protección de pérdida de acceso por descuido

El sistema asegura que en el proyecto permanezca configurado siempre al menos un usuario del tipo "Administrator". Con esto se evita que el acceso a un proyecto se pueda perder irrecuperablemente por un "autoborrado" no intencionado.

ATENCIÓN
Si se modifican los ajustes de la autenticación, se tienen que cargar de nuevo los módulos SCALANCE S para que se activen estos ajustes (p. ej. nuevos usuarios, cambios de contraseña) en los módulos.

4.4.4 Check Consistency

Resumen

Security Configuration Tool distingue:

- Pruebas de coherencia locales
- Pruebas de coherencia a nivel de proyecto

Encontrará información sobre las reglas comprobadas que debe tener en cuenta al realizar entradas en los cuadros de diálogo en las descripciones de los diálogos que aparecen en el manual bajo el término clave "Check Consistency" (prueba de coherencia).

Pruebas de coherencia locales

Una prueba de coherencia se considera local si se puede realizar directamente dentro de un diálogo. Se pueden producir comprobaciones con motivo de las siguientes acciones:

- al salir de un campo
- al salir de una fila en una tabla
- al salir del cuadro de diálogo con "OK" ("Aceptar").

Pruebas de coherencia a nivel de proyecto

Las pruebas de coherencia a nivel de proyecto informan sobre la configuración correcta de módulos. Ya que las pruebas continuas de coherencia de todo el proyecto llevan demasiado tiempo porque durante la creación de un proyecto se configuran la mayoría de las veces datos de proyecto inconsistentes, se realiza automáticamente una prueba sólo en las siguientes acciones:

- al guardar el proyecto
- al abrir el proyecto
- antes de cargar una configuración

ATENCIÓN
Sólo se pueden cargar datos de proyecto si el proyecto es coherente en su conjunto.

Así puede impulsar una prueba de coherencia a nivel de proyecto

Puede impulsar en todo momento una prueba de coherencia para un proyecto abierto a través del siguiente comando de menú:

Options ▸ Check Consistency

El resultado de la prueba se presenta en una lista. Adicionalmente se hace referencia al resultado de la prueba de coherencia en la barra de estado, si el proyecto contiene datos incoherentes. Poniendo el puntero del ratón en la barra de estado puede visualizar entonces la lista de pruebas haciendo un clic.

4.4.5 Asignación de nombre simbólicos para direcciones IP o MAC

Significado y ventaja

En un proyecto SCALANCE S puede asignar, en una tabla de símbolos, nombres simbólicos en representación de direcciones IP o MAC.

La configuración de los distintos servicios se puede realizar así de manera sencilla y segura.

En el caso de las siguientes funciones y su configuración se tienen en cuenta nombres simbólicos dentro del proyecto:

- Firewall
- Router NAT/NAPT
- Syslog
- DHCP

Validez y carácter inequívoco

La validez de los nombres simbólicos indicados en la tabla de símbolos está limitada a la configuración dentro de un proyecto SCALANCE S.

Dentro del proyecto, cada nombre simbólico ha de estar asignado de forma inequívoca a una única dirección IP o MAC.

Transferencia automática de nombres simbólicos a la tabla de símbolos

Puede utilizar nombres simbólicos en lugar de direcciones IP en las funciones mencionadas, por ejemplo al crear reglas de firewall, sin que dichos nombres estén asignados ya en la tabla de símbolos aquí descrita.

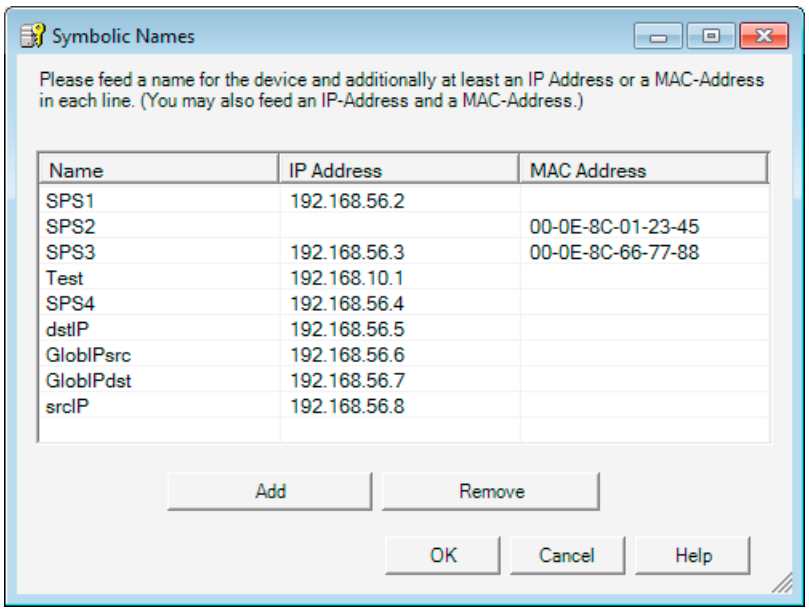
Nombres simbólicos así asignados se transfieren automáticamente a la tabla de símbolos y se puede establecer la correspondencia en un momento ulterior. En el marco de la prueba de la coherencia se advierte de la falta de correspondencia.

Cuadro de diálogo para asignación de nombres simbólicos

Para evitar una incoherencia en ua correspondencia "Dirección IP - Nombre simbólico" así como "Dirección MAC - Nombre simbólico", los nombres simbólicos se administran en una sola tabla de símbolos.

Seleccione el siguiente comando para abrir la tabla de símbolos:

Options ▸ Symbolic Names..



Proceda del siguiente modo para realizar entradas en la tabla de símbolos:

- **Nuevas entradas**

1. Pulse el botón "Add" para añadir un nuevo nombre simbólico en la siguiente línea libre de la tabla.
2. Introduzca el nombre simbólico conforme a DNS. [1)]
3. Complete la entrada con la dirección IP o MAC. También puede introducir ambas direcciones.

Leyenda:

[1)] La conformidad con DNS según RFC1035 comprende las siguientes reglas:
- limitación a 255 caracteres en total (letras, cifras, guión o punto);
- el nombre tiene que comenzar con una letra;
- el nombre sólo puede terminar con una letra o una cifra;
- un componente dentro del nombre, es decir, una cadena de caracteres entre dos puntos, debe tener una longitud máxima de 63 caracteres;
- no se permiten caracteres especiales como diéresis, paréntesis, subrayados, espacios, etc.

- **Entradas automáticas**

Si el nombre simbólico se ha introducido ya en el marco de un servicio, encontrará la entrada correspondiente en la tabla de símbolos.

1. Haga clic en el campo de entrada para la dirección IP o la dirección MAC.
2. Complete la entrada con la dirección IP o MAC. También puede introducir ambas direcciones.

Si borra una entrada de la tabla de símbolos, los nombres simbólicos utilizados en los servicios siguen existiendo en los mismos. En tales casos, la prueba de coherencia reconoce nombres simbólicos no definidos. Esto es válido tanto para entradas realizadas manualmente como para las generadas de modo automático.

Un consejo:

Para la tabla de símbolos aquí descrita es particularmente conveniente la aplicación de una prueba de coherencia a nivel de proyecto. En base a la lista se pueden detectar y corregir irregularidades.

Puede impulsar en todo momento una prueba de coherencia para un proyecto abierto a través del siguiente comando de menú:

Options ▸ Check Consistency

Prueba de coherencia - reglas a considerar

Al realizar sus entradas debe tener en cuanta las reglas indicadas a continuación.

Prueba / Regla	Prueba realizada [1]	
	a nivel local	a nivel de proyecto
La asignación de un nombre simbólico a una dirección IP o MAC tiene que ser inequívoca en ambos sentidos.	X	
Los nombre simbólicos han de ser conformes con DNS. [2]	X	
Cada línea de la tabla de símbolos tiene que contener un solo nombre simbólico. Tiene que estar indicada una dirección IP, una dirección MAC o ambas.	X	
No se deben asignar nombres simbólicos a las direcciones IP de los módulos SCALANCE S.		X
Nombre simbólicos utilizados en el proyecto para direcciones IP o MAC tienen que estar incluidos en la tabla de símbolos. Se pueden producir incoherencias si se borran entradas de la tabla de símbolos y no se eliminan o corrigen correspondientemente en los cuadros de diálogo del proyecto.		X

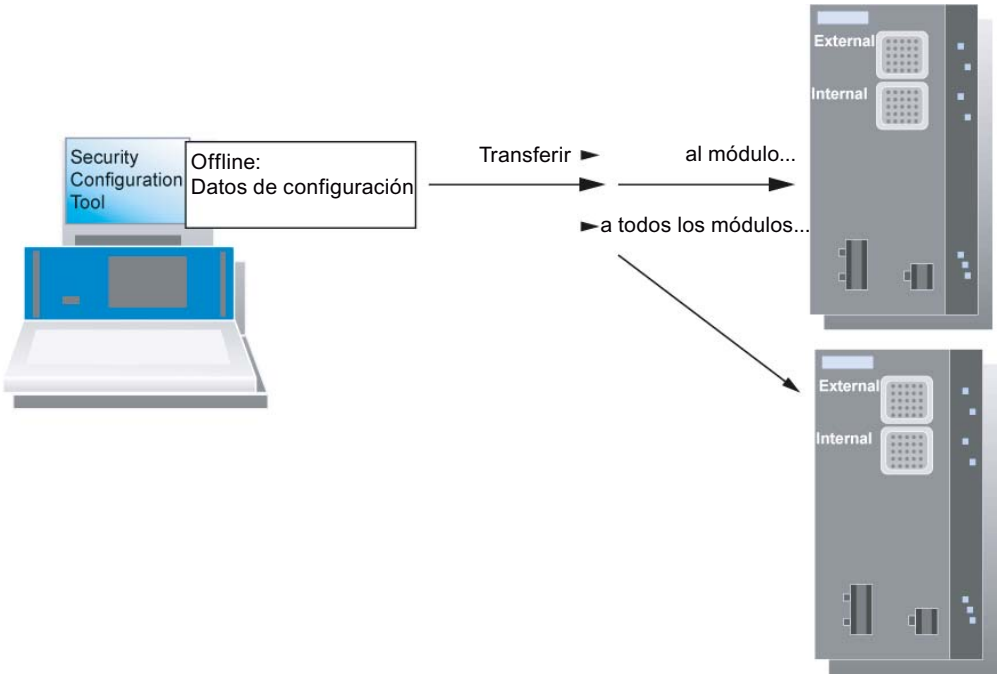
Leyenda:

[1] Observe las explicaciones del capítulo "Pruebas de coherencia".

[2] La conformidad con DNS según RFC1035 comprende las siguientes reglas:
- limitación a 255 caracteres en total (letras, cifras, guión o punto);
- el nombre tiene que comenzar con una letra;
- el nombre sólo puede terminar con una letra o una cifra;
- un componente dentro del nombre, es decir, una cadena de caracteres entre dos puntos, debe tener una longitud máxima de 63 caracteres;
- no se permiten caracteres especiales como diéresis, paréntesis, subrayados, espacios, etc.

4.5 Cargar la configuración en SCALANCES S

Los datos de configuración creados offline se cargan con los correspondientes comandos de menú en los SCALANCE S accesibles en la red.



Requisitos

- Conexiones

  En principio, los datos de configuración se pueden cargar tanto a través del puerto 1 como del puerto 2 del equipo.

  Configure preferentemente los módulos de un grupo a través de la red externa común de esos módulos (puerto 1 del equipo).

  Si el ordenador de configuración se encuentra en una red interna, se tienen que liberar explícitamente en el firewall de ese SCALANCE S las direcciones IP de los demás módulos del grupo, configurando luego el módulo en cuestión en primer lugar. (Se soporta este procedimiento si ya se les ha asignado una dirección IP a todos los módulos SCALANCE S. Vea "Peculiaridades de la primera configuración")

ATENCIÓN
Utilizar múltiples adaptadores de red durante la primera configuración
Si utiliza varios adaptadores de red en su PC/PG, seleccione primero, antes de la primera configuración, el adaptador de red a través del que desea acceder al módulo SCALANCE S.
Utilice para ello el comando "**Options▸ Network Adapter…**"

- Estado operativo

  Configuraciones se pueden cargar durante el funcionamiento normal de los equipos SCALANCE S. Tras el proceso de carga tiene lugar automáticamente un rearranque de los equipos. Después de la carga se puede producir una breve interrupción de la comunicación entre la red interna y la externa.

ATENCIÓN
Peculiaridades de la primera configuración
Mientras en un módulo no se hayan ajustado parámetros IP (es decir, antes de la primera configuración), no se debe encontrar ningún router o SCALANCE S entre el módulo y el ordenador de configuración.

ATENCIÓN
Cambio de la conexión de PC
Si se pasa un PC del puerto interno al externo del SCALANCE S, los accesos de este PC al SCALANCE S se bloquean durante un plazo de 10 minutos aproximadamente (función de seguridad para proteger de "ARP-Cache-Spoofing").

ATENCIÓN
El proyecto tiene que ser coherente
Sólo se pueden cargar datos de proyecto si el proyecto es coherente en su conjunto. En caso de incoherencia se muestra una lista de pruebas detallada.

Transmisión segura

Los datos se transmiten con un protocolo seguro.

Procedimiento a seguir

Como alternativa, utilice para la carga los comandos de menú:

- **Transfer ▸ To Module...**

  Transfiera con esto la configuración a todos los módulos seleccionados.

- **Transfer ▸ To All Modules…**

  Transfiera con esto la configuración a todos los módulos configurados en el proyecto.

Asimilación de configuraciones distintas

No es posible recargar en el proyecto datos de configuración del módulo SCALANCE S.

4.6 Datos de configuración para MD 740 / MD 741

Transmisión a un módulo

Puede generar sus informaciones de VPN para la parametrización de un MD 740-1 / MD 741-1 con la Security Configuration Tool. Con los archivos así generados puede configurar entonces el MD 740-1 / MD 741-1.

Se generan los siguientes tipos de archivos:

- Archivo de exportación con los datos de configuración
  - Tipo de archivo: archivo ".txt" en formato ASCII
  - Contiene las informaciones sobre configuración exportadas para el MD 740 / MD 741, inclusive una información sobre los certificados generados adicionalmente.
- Certificado de módulo
  - Tipo de archivo: Archivo ".p12"
  - El archivo contiene el certificado de módulo y el material de clave.
  - El acceso está protegido por contraseña.
- Certificado de grupo
  - Tipo de archivo: Archivo ".cer"

Los archivos de configuración para el MD 740-1 / MD 741-1 se pueden utilizar también para configurar otros tipos de VPN Client no incluidos en la selección de módulos. El requisito mínimo para el uso de estos VPN Clients es la compatibilidad con IPsec VPNs en el modo de túnel.

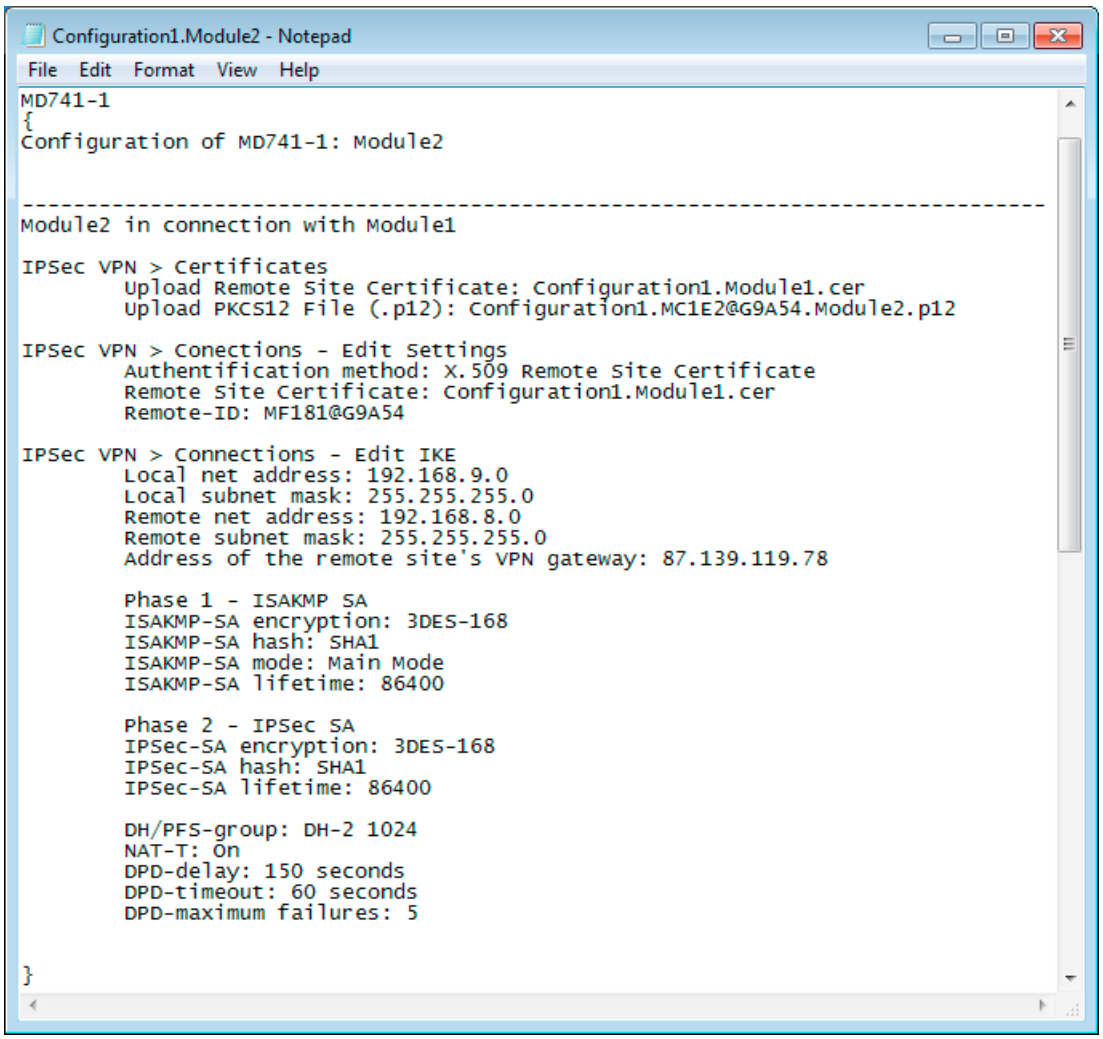


Figura 4-1 Archivo de exportación para MD 741-1

Nota

No se transmite ningún archivo de configuración al módulo. Sólo se genera un archivo ASCII con el que se puede configurar el MD 740-1 / MD 741-1. Pero esto sólo es posible si el módulo se encuentra en al menos un grupo VPN en el que exista también un módulo SCALANCE S o un SOFTNET Security Client V3.0.

Proceda del siguiente modo

1. Marque en el módulo "MD 740-1" / "MD 741-1" y seleccione **Transfer ▸ To Module...**.
2. Introduzca en el siguiente diálogo para almacenamiento la ruta y el nombre del archivo de configuración y haga clic en "Save".
3. A continuación se le pregunta si quiere crear una contraseña propia para los dos archivos de certificado generados.

   Si responde "No", se asigna como contraseña el nombre de la configuración (p. ej. DHCP_ohne_Routing_02), y no la contraseña del proyecto.

   Si responde "Yes" (recomendado), tiene que introducir su contraseña en el diálogo subsiguiente.

   Resultado: Los archivos (y certificados) se guardan en el directorio indicado por usted.

Nota

Después de guardar se le advierte de que el proyecto es incompatible hacia abajo. Proyectos guardados, por ejemplo, con la Security Configuration Tool V2.1 no se pueden cargar con la Security Configuration Tool V2.

Nota

Podrá encontrar más información para la configuración del MD 740-1 / MD 741-1 en el Manual de sistema MD 741-1 / MD 740-1.

Firewall, Router y otras propiedades del módulo 5

El presente capítulo le familiariza con la creación de módulos y con los ajustes que se pueden efectuar en un proyecto para los distintos módulos. El papel principal lo desempeñan al respecto los ajustes correspondientes a la función Firewall y la función NAT/NAPT Router del SCALANCE S.

Nota

S612/S613

Los ajustes de firewall que se pueden efectuar para los distintos módulos pueden influir también en la comunicación que se desarrolla a través de conexiones túnel IPsec en la red interna (VPN).

Otras informaciones

La configuración de túneles IPsec se describe con detalle en el capítulo siguiente de este manual.

La ayuda online le proporcionará también información detallada sobre los diálogos y los parámetros ajustables.

Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

ATENCIÓN
Prestaciones y tipos de equipos Tenga en cuenta cuáles son las funciones a las que da soporte el tipo de equipo utilizado por usted.

Consulte también

Funciones online - Test, Diagnóstico y Logging (Página 221)

Características de hardware y panorámica de las funciones (Página 17)

5.1 Vista general / principios

5.1.1 SCALANCE S como firewall

Significado

La función Firewall del SCALANCE S tiene la misión de proteger la red interna de influencias o perturbaciones procedentes de la red externa. Esto significa que, dependiendo de la configuración, sólo se permiten determinadas relaciones de comunicación, previamente definidas, entre nodos de la red interna y nodos de la red externa.

Todos los nodos de red que se encuentran en el segmento de red interno de un SCALANCE S son protegidos por su firewall.

Las funciones de Firewall se pueden configurar para los siguientes niveles de protocolo:

- IP-Firewall con Stateful Packet Inspection;
- Firewall también para telegramas Ethernet-"Non-IP" según IEEE 802.3; (telegramas Layer 2)
- Limitación del ancho de banda

Reglas de Firewall

Las reglas de Firewall son reglas para el tráfico de datos en los siguientes sentidos:

- de red interna a externa y viceversa;
- de red interna a un túnel IPsec y viceversa (S612/S613).

Configuración

Se deben distinguir los dos vistas de operación:

- En Standard Mode se recurre a reglas sencillas, predefinidas.
- En el Advanced Mode puede definir reglas específicas.

  Adicionalmente, en el Advanced Mode se puede distinguir entre reglas de Firewall locales y reglas de Firewall globales para módulos:

  – Reglas de Firewall locales están asignadas a un módulo en cada caso. Se configuran en el diálogo de propiedades de los módulos.

  – Las reglas globales para firewall se pueden asignar a varios módulos a un tiempo. Esta posibilidad simplifica en muchos casos la configuración.

Adicionalmente se tiene la posibilidad de definir reglas de firewall de forma compacta y clara con ayuda de definiciones de servicios. Estas definiciones de servicios se pueden tomar como referencia tanto para reglas de Firewall locales como para bloques de reglas de Firewall globales.

5.1.2 SCALANCE S como Router

Significado

Utilizando SCALANCE S como router conecta la red interna con la red externa. La red interna conectada a través de SCALANCE S se convierte así en una subred propia.

Tiene las siguientes posibilidades:

- Routing - ajustable en Standard Mode y Advanced Mode
- NAT/NAPT-Routing - ajustable en Advanced Mode

Routing - ajustable en Standard Mode y Advanced Mode

Se transmiten los telegramas dirigidos a una dirección IP existente en la respectiva subred (interna o externa). Por lo demás son válidas las reglas de Firewall adoptadas para el respectivo sentido de transmisión.

Para este modo de operación se tiene que configurar adicionalmente una dirección IP para la subred interna.

Nota: A diferencia del modo Bridge del SCALANCE S, en el modo Routing se pierden VLAN-Tags.

NAT/NAPT-Routing - ajustable en Advanced Mode

En este modo de operación tiene lugar además una conversión de las direcciones IP. Las direcciones IP de los equipos de la subred interna se representan en direcciones IP de la red externa, con lo que no son "visibles" en la red externa.

Para este modo de operación tiene que configurar la conversión de dirtecciones en una lista. Asigne en cada caso una dirección IP externa a una dirección IP interna.

Dependiendo del método que desee utilizar, rige para la correspondencia:

- NAT (Network Adress Translation)

  Aquí rige: Dirección = Dirección IP
- NAPT (Network Address Port Translation)

  Aquí rige: Dirección = Dirección IP + Número de puerto

5.1.3 SCALANCE S como DHCP-Server

Significado

Puede utilizar SCALANCE S como DHCP-Server en la red interna. Esto permite asignar automáticamente direcciones IP a los equipos conectados a la red interna.

Las direcciones se asignan en este caso dinámicamente, desde una banda de direcciones definida por usted, o bien se asigna una dirección IP a un equipo concreto conforme a sus predeterminaciones.

Configuración

La configuración como DHCP-Server es posible en la vista "Advanced Mode".

5.2 Crear módulos y ajustar parámetros de red

Crear módulos

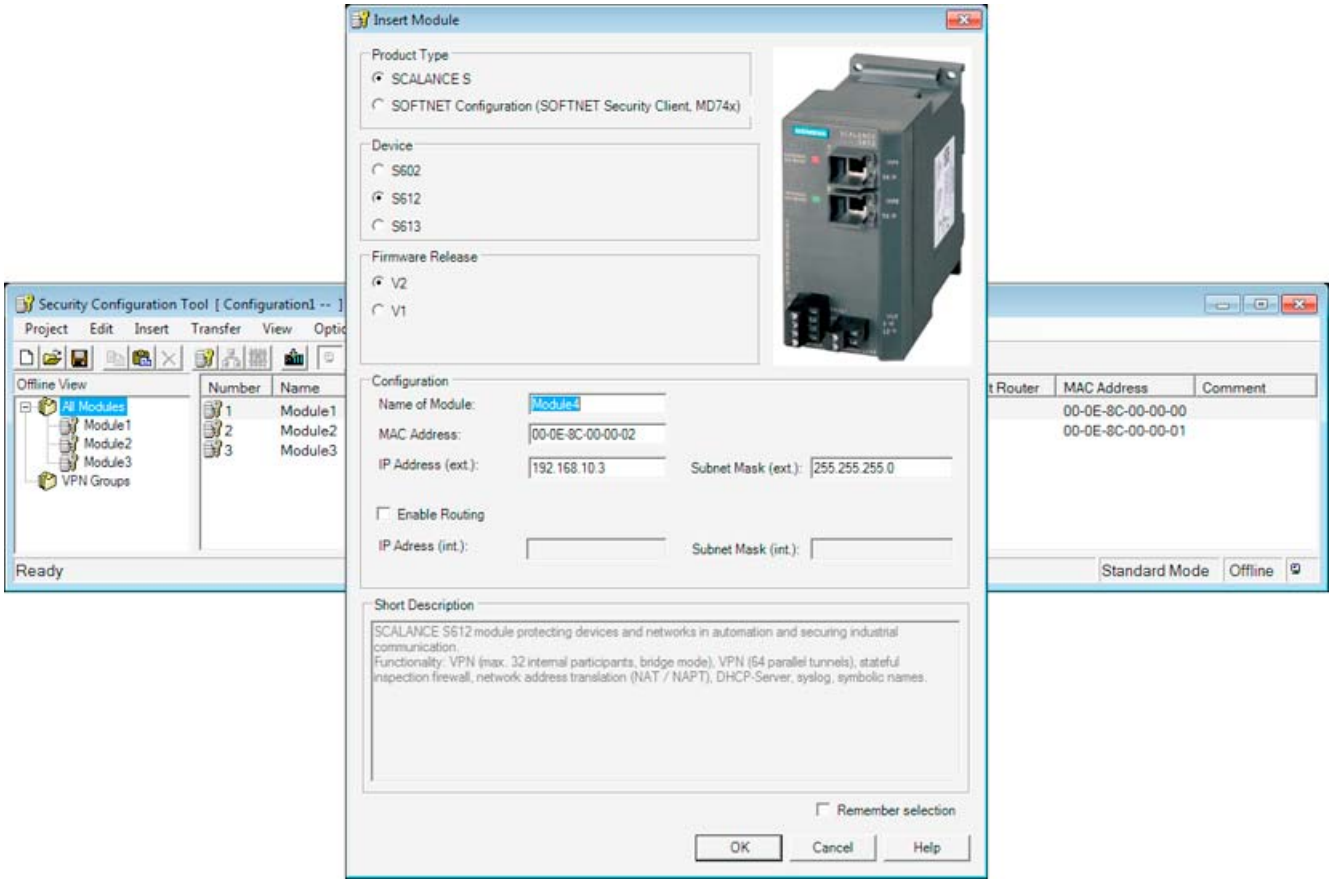
Al crear un nuevo proyecto, la Security Configuration Tool abre de forma estándar el cuadro de diálogo "Selección de un módulo o configuración de software", en el que usted puede configurar su primer módulo.

Con el comando de menú siguiente se crean otros nuevos módulos:

Insert ▸ Module

alternativa: a través del menú de contexto, estando seleccionado el objeto "All Modules".

Seleccione en el siguiente paso de este cuadro de diálogos, su tipo de producto, el módulo y la versiónde firmware.



Ajustes de red de un módulo

Los ajustes de red de un módulo abarcan:

- Parámetros de dirección del módulo
- Direcciones de routers externos

Parámetros de dirección

Puede usted configurar los parámetros de dirección a través del cuadro de diálogo "Selección de un módulo o configuración de software" al crear un módulo.

Los parámetros de dirección se pueden introducir también en el área de contenido, seleccionando para ello en el área de navegación el objeto "All Modules":

Se visualizan por columnas las siguientes propiedades de los módulos:

Tabla 5- 1 Parámetros IP - "All Modules" seleccionado

Propiedad/columna	Significado	Comentario/selección
Nummer	Número de módulo correlativo	se asigna automáticamente
Name	Denominación del módulo tecnológicamente razonable.	de libre elección
Dirección IP ext.	Dirección IP a través de la cual se puede acceder al equipo en la red externa, por ejemplo para cargar la configuración.	Asignación adecuada para la red.
Máscara de subred ext.	Máscara de subred	Asignación adecuada para la red.
Dirección IP int.	Dirección IP a través de la cual se puede acceder al equipo en la red interna, por ejemplo si está configurado como router.	Asignación adecuada para la red. Este campo de entrada sólo se puede editar si en las propiedades del módulo se ha activado el modo Router.
Máscara de subred int.	Máscara de subred	Asignación adecuada para la red. Este campo de entrada sólo se puede editar si en las propiedades del módulo se ha activado el modo Router.
Default Router	Dirección IP del router en la red externa.	Asignación adecuada para la red.
Dirección MAC	Dirección de hardware del módulo	La dirección MAC está impresa en la carcasa del módulo. • Tenga en cuenta la dirección MAC adicional en el modo Routing (datos a continuación de esta tabla).

Propiedad/columna	Significado	Comentario/selección
Type	Tipo de equipo	• SCALANCE S602 • SCALANCE S612 V1 • SCALANCE S612 V2 • SCALANCE S613 V1 • SCALANCE S613 V2
		• SOFTNET Security Client 2005 • SOFTNET Security Client 2008 • SOFTNET Security Client V3.0 • MD 74x Para estos tipos de módulos no existe ningún "diálogo de propiedades". Para MD 74x se pueden ajustar en la zona del contenido las direcciones IP y las máscaras de subred.
Comentario	Información tecnológicamente lógica sobre el módulo y la subred protegida por el módulo.	de libre elección

Dirección MAC adicional en el modo Routing

SCALANCE S utiliza en el modo Routing una dirección MAC adicional en la interfaz para la subred interna. Esta segunda dirección MAC se deriva del modo aquí descrito de la dirección MAC impresa en el equipo:

- Dirección MAC (interna) = Dirección MAC impresa + 1

Si se trabaja en redes planas (modo Bridge), la dirección MAC impresa es válida siempre tanto en la interfaz interna como en la externa.

En el diálogo Online de la Security Configuration Tool se muestran las direcciones MAC actualmente válidas en la ficha "Status".

Cuadro de diálogo "Network / External Routers"

Dependiendo de la estructura de red existente, puede suceder que además del router predeterminado tenga que indicar otros routers.

Marque el módulo a editar y seleccione el siguiente comando de menú para configurar routers externos:

Edit ▸ Properties..., ficha "Network"

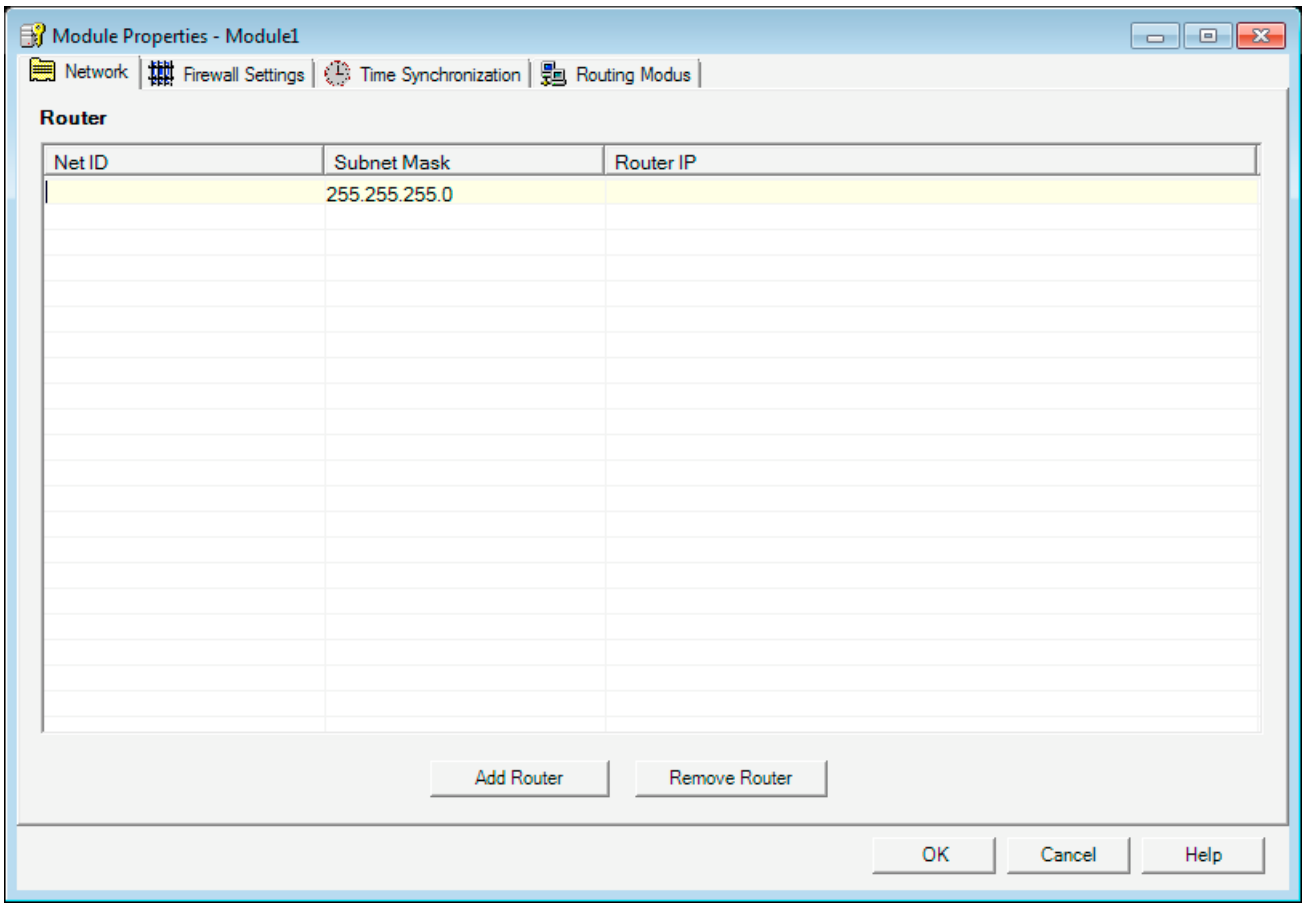


Figura 5-1 Diálogo "Network"

Consulte también

Panorámica de funciones del cuadro de diálogo online (Página 222)

5.3 Firewall - Propiedades del módulo en el Standard Mode

5.3.1 Configurar firewall

Protección de perturbaciones procedentes de la red externa

La función Firewall del SCALANCE S tiene la misión de proteger la red interna de influencias o perturbaciones procedentes de la red externa. Esto significa que sólo se permiten determinadas relaciones de comunicación, previamente definidas, entre nodos de la red interna y nodos de la red externa.

Con reglas para filtrado de paquetes se define la liberación o la restricción del tráfico de datos en tránsito, sobre la base de propiedades de los paquetes de datos.

En SCALANCE S612 / S613 , el firewall se puede utilizar para el tráfico de datos codificado (túnel IPsec) y el no codificado.

En el modo Standard sólo se pueden realizar ajustes para el tráfico de datos no codificado.

Nota

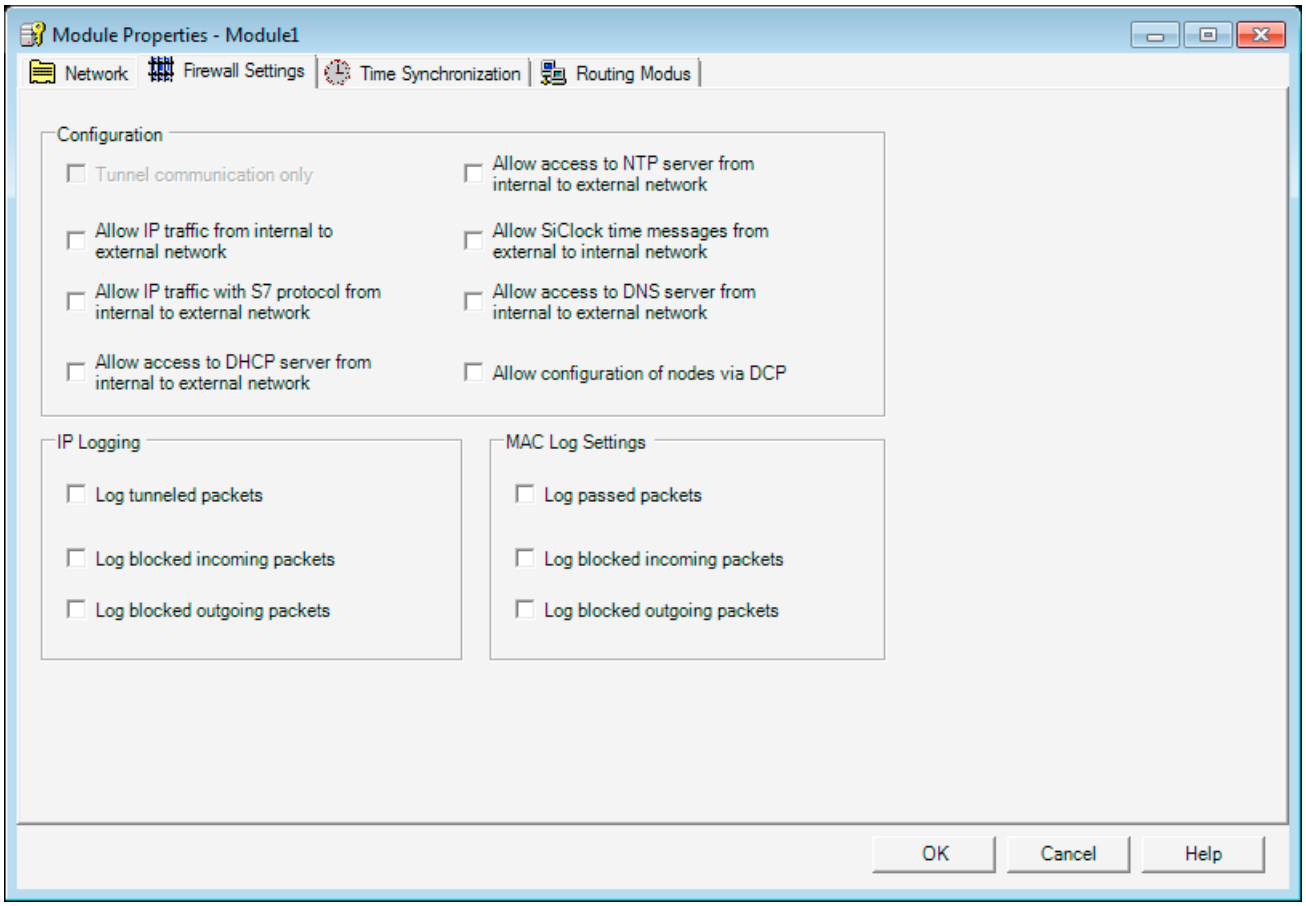
Routing Modus

Si ha activado el modo Routing para el módulo SCALANCE S, no tienen aplicación las reglas de MAC.

Cuadro de diálogo

Marque el módulo a editar y seleccione el siguiente comando de menú para configurar el firewall:

Edit ▸ Properties..., ficha "Firewall"


Module Properties - Module1
Network
Firewall Settings
Time Synchronization
Routing Modus
Configuration
Tunnel communication only
Allow access to NTP server from internal to external network
Allow IP traffic from internal to external network
Allow SiClock time messages from external to internal network
Allow IP traffic with S7 protocol from internal to external network
Allow access to DNS server from internal to external network
Allow access to DHCP server from internal to external network
Allow configuration of nodes via DCP
IP Logging
Log tunneled packets
Log blocked incoming packets
Log blocked outgoing packets
MAC Log Settings
Log passed packets
Log blocked incoming packets
Log blocked outgoing packets
OK
Cancel
Help

Campo de selección "Configuration" - Reglas predefinidas

ATENCIÓN
Tenga en cuenta que el potencial de riesgo se hace mayor cuanto más opciones se habilitan.

El Standard Mode contiene para el firewall las siguientes reglas predefinidas, que puede seleccionar en el área de entrada "Configuration":

Tabla 5- 2 Reglas predefinidas del firewall simple

Regla/opción	Función	Ajuste Default
Sólo comunicación por túnel (S612/ S613) Tunnel Communication only	Éste es el ajuste predeterminado. Con este ajuste sólo se permite la transferencia codificada de datos por IPsec; sólo nodos de la red interna de SCALANCE S pueden comunicarse entre sí. La opción sólo se puede seleccionar si el módulo se encuentra en un grupo. Si esta opción está desactivada, se permite la comunicación por túnel y adicionalmente el tipo de comunicación seleccionado en las otras casillas de opción.	on
Erlaube IP-Verkehr vom internen ins externe Netz Allow outgoing IP traffic	Nodos internos pueden iniciar una comunicación con nodos de la red externa. Sólo se transmiten a la red interna telegramas de respuesta procedentes de la red externa. Desde la red externa no se puede iniciar ninguna comunicación con nodos de la red interna.	off
Erlaube IP-Verkehr mit S7-Protokoll vom internen ins externe Netz. Allow outgoing S7 protocol	Nodos internos pueden iniciar una comunicación S7 (protocolo S7 - TCP/Port 102) con nodos de la red externa. Sólo se transmiten a la red interna telegramas de respuesta procedentes de la red externa. Desde la red externa no se puede iniciar ninguna comunicación con nodos de la red interna.	off
Erlaube Zugriff auf DHCP-Server vom internen ins externe Netz. Allow access to external DHCP server	Nodos internos pueden iniciar una comunicación con un servidor DHCP de la red externa. Sólo los telegramas de respuesta del servidor DHCP se transmiten a la red interna. Desde la red externa no se puede iniciar ninguna comunicación con nodos de la red interna.	off
Erlaube Zugriff auf NTP-Server vom internen ins externe Netz. Allow access to external NTP server	Nodos internos pueden iniciar una comunicación con un servidor NTP (Network Time Protocol) de la red externa. Sólo los telegramas de respuesta del servidor NTP se transmiten a la red interna. Desde la red externa no se puede iniciar ninguna comunicación con nodos de la red interna.	off
Erlaube SiClock-Uhrzeittelegramme vom externen ins interne Netz. Allow access to external SiClock server	Con esta opción se habilitan telegramas horarios SiClock de la red externa a la interna.	off (Esta opción no se puede utilzar en el modo Routing.)

Regla/opción	Función	Ajuste Default
Erlaube Zugriff auf DNS-Server vom internen ins externe Netz. Allow access to external DNS server	Nodos internos pueden iniciar una comunicación con un servidor DNS de la red externa. Sólo los telegramas de respuesta del servidor DNS se transmiten a la red interna. Desde la red externa no se puede iniciar ninguna comunicación con nodos de la red interna.	off
Erlaube die Konfiguration von internen Netzknoten mittels DCP vom externen ins interne Netz. Allow access from external or internal nodes via DCP server	El protocolo DCP es utilizado por la PST-Tool para realizar, en el caso de componentes de red SIMATIC Net, el bautismo de nodos (ajuste de los parámetros IP). Con esta regla se permite a nodos de la red externa acceder a nodos de la red interna mediante protocolo DCP.	off (Esta opción no se puede utilzar en el modo Routing.)

Campo de selección "Log" - Ajustar registro

Puede proveer una protolización a través del tráfico de datos entrante o saliente.

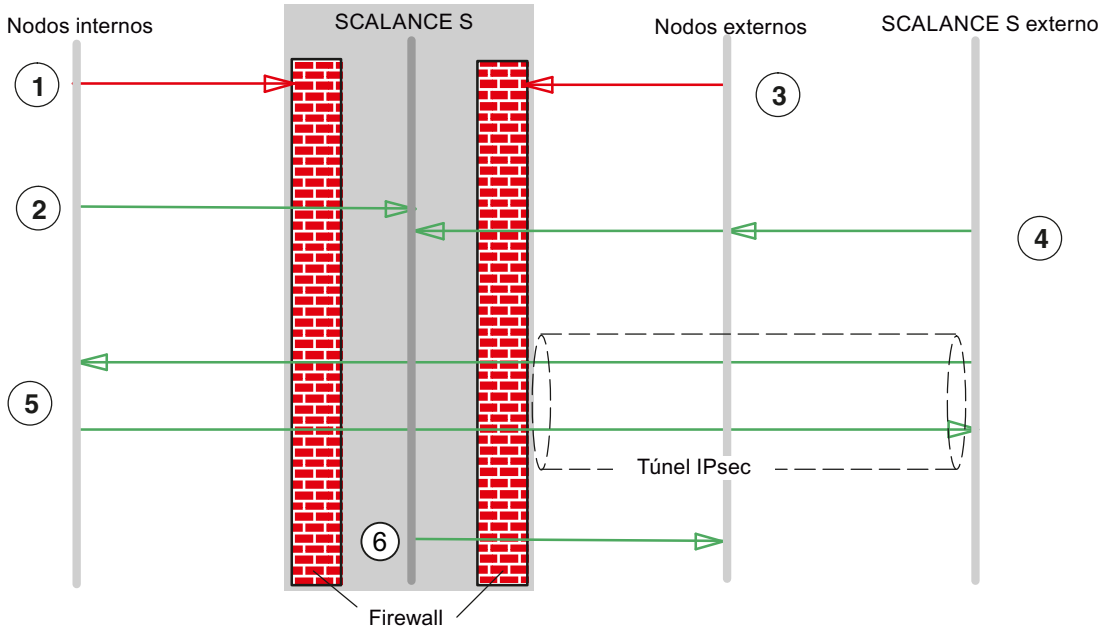
5.3.2 Preajuste del firewall

Comportamiento con preajuste

El preajuste del firewall se ha elegido de forma que no sea posible tráfico de datos IP. Sólo a través de un túnel IPsec eventualmente configurado se permite la comunicación entre los nodos de la red interna de módulos SCALANCE S.

Los diagramas siguientes muestran en detalle los ajustes estándar para el filtro de paquetes IP y el filtro de paquetes MAC.

Ajuste predeterminado para filtro de paquetes IP

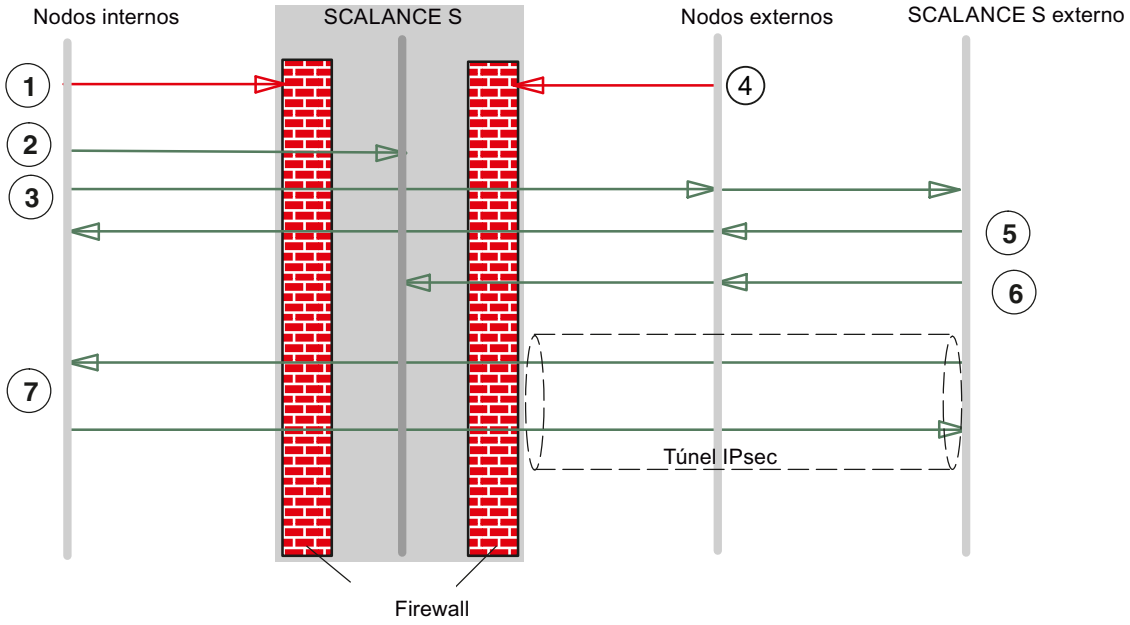


① Todos los tipos de telegramas de interno a externo están bloqueados.
② Todos los telegramas de interno a SCALANCE S están permitidos (conveniente sólo para HTTPS).
③ Todos los telegramas de externo a interno y a SCALANCE S están bloqueados (también ICMP-Echo-Request).
④ Se permiten telegramas de externo (nodo externo y SCALANCE S externo) a SCALANCE S del siguiente tipo:

- HTTPS (SSL)
- Protocolo ESP (codificación)
- IKE (protocolo para establecer el túnel IPsec)
- NAT-Traversal (protocolo para establecer el túnel IPsec)

⑤ La comunicación IP por el túnel IPsec está permitida.
⑥ Telegramas del tipo Syslog y NTP sólo se permiten de SCALANCE S a externo.

Ajuste predeterminado para filtro de paquetes MAC



① Todos los tipos de telegramas de interno a externo están bloqueados.
② Todos los telegramas de interno a SCALANCE S están permitidos.
③ Los telegramas ARP de interno a externo están permitidos.
④ Todos los telegramas de externo a interno y a SCALANCE S están bloqueados.
⑤ Se permiten telegramas de externo a interno del siguiente tipo:
- ARP con limitación de ancho de banda

⑥ Se permiten telegramas de externo a SCALANCE S del siguiente tipo:
- ARP con limitación de ancho de banda
- DCP

⑦ Se permiten protocolos MAC enviados por túnel IPsec.

5.4 Firewall - Propiedades del módulo en el Advanced Mode

En el Advanced Mode existen otras posibilidades de ajuste que permiten ajustar de forma personalizada las reglas de firewall y las funciones de seguridad.

Conmmutar al Advanced Mode

Para todas las funciones descritas en este capítulo, conmute el modo de funcionamiento con el siguiente comando de menú:

View ▸ Advanced Mode...

Nota

Una conmutación realizada al Advanced Mode para el proyecto actual ya no se puede anular en cuanto se haya modificado la configuración.

Se da soporte a nombres simbólicos

En las funciones descritas a continuación puede introducir tanto direcciones IP o MAC como nombres simbólicos.

5.4.1 Configurar firewall

A diferencia de la configuración de reglas de filtrado de paquetes predeterminadas de forma fija en el Standard Mode, en el Advanced Mode se pueden configurar con la Security Configuration Tool reglas de filtrado de paquetes peronalizadas.

Las reglas de filtrado de paquetes se ajustan en fichas seleccionables para los siguientes protocolos:

- Protocolo IP (Nivel/Layer 3)
- Protocolo MAC (Nivel/Layer 2)

Si no introduce ninguna regla en los cuadros de diálogo que se describen a continuación, rigen los ajustes predeterminados conforme a lo descrito en el capítulo "Preajuste del Firewall".

Nota

Routing Modus

Si ha activado el modo Routing para el módulo SCALANCE S, no tienen aplicación las reglas de MAC (los diálogos están inactivos).

Es posible la definición global y local

- Reglas de Firewall globales

  Una regla global para firewall se puede asignar a varios módulos a un tiempo. Esta posibilidad simplifica en muchos casos la configuración.

- Reglas de Firewall locales

  Una regla de firewall local está asignada a un módulo en cada caso. Se configura en el diálogo de propiedades de un módulo.

A un módulo se le pueden asignar varias reglas de firewall locales y varias reglas de firewall globales.

La definición de reglas globales y locales tiene lugar, en principio, de forma idéntica. La descripción siguiente es válida pues para los dos métodos citados.

5.4.2 Reglas de Firewall globales

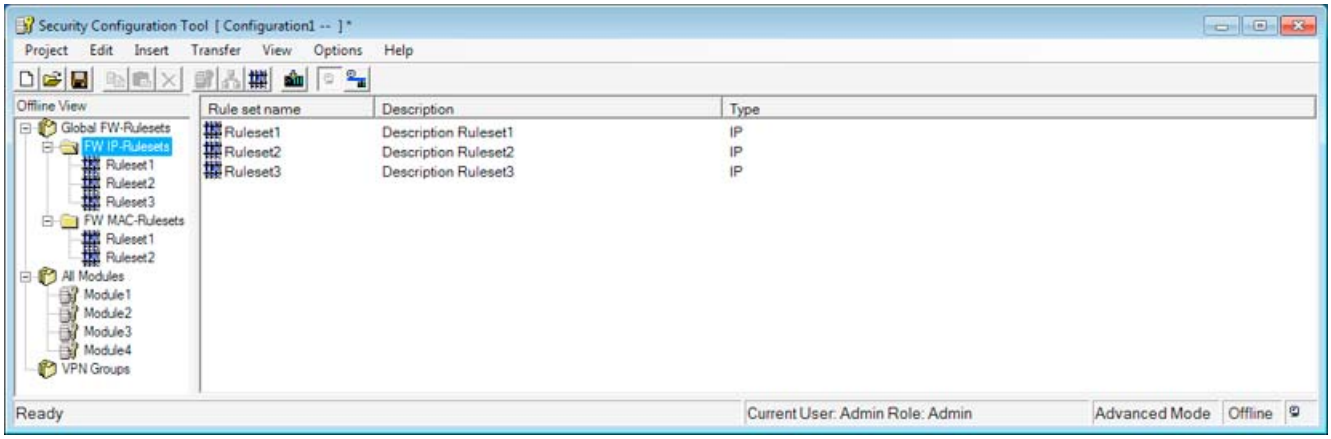
Aplicación

Las reglas de firewall globales se configuran fuera de los módulos, a nivel de proyecto. Análogamente al caso de los módulos, se pueden ver en el área de navegación de la Security Configuration Tool.

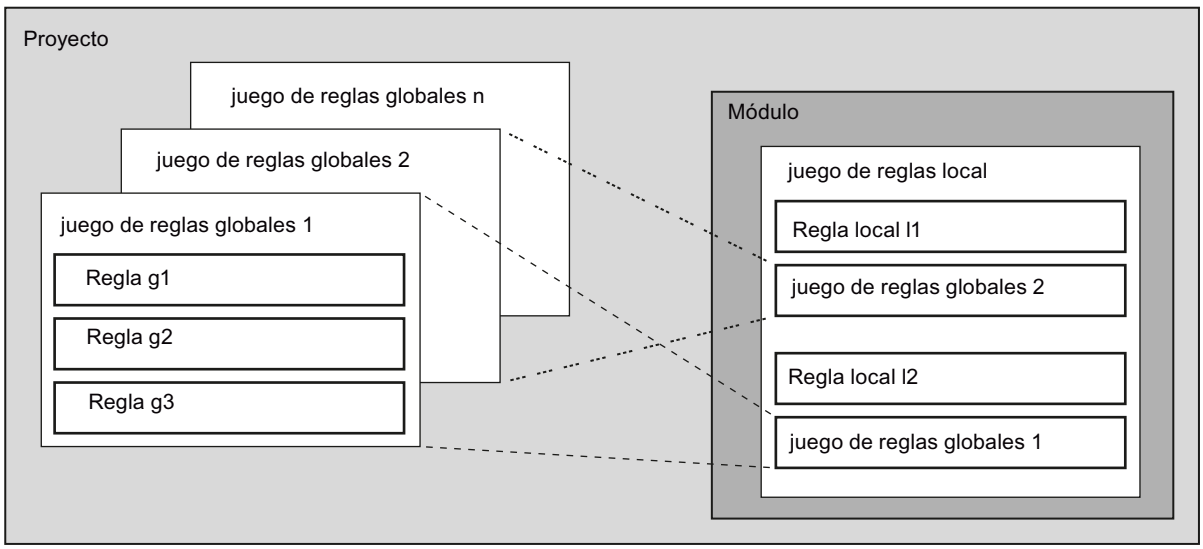
Seleccionando un módulo configurado y arrastrándolo a la regla de Firewall global ("Drag and Drop"), se asigna esa regla de Firewall a ese módulo. Esta regla de Firewall global aparece entonces automáticamente en la lista de reglas de Firewall específica del módulo.

Se pueden definir reglas de Firewall globales para:

- bloques de reglas IP
- bloques de reglas MAC



La representación siguiente ilustra la relación entre los bloques de reglas de definición global y los bloques de reglas utilizados a nivel local.



¿Cuándo son convenientes reglas de Firewall globales?

El uso de reglas de Firewall globales tiene sentido si puede definir criterios de filtro idénticos para la comunicación de varias subredes protegidas por módulos SCALANCE S con la red externa.

Debe tener en cuenta, sin embargo, que esta configuración simplificada puede conducir a resultados no deseados en caso de una asignación incorrecta de los módulos. Por ello debería comprobar siempre los resultados de las reglas de Firewall locales específicas del módulo. Una asignación de reglas efectuada por descuido no se puede reconocer en el marco de la prueba automática de la coherencia.

Las reglas de Firewall globales se utilizan localmente - convenios

Rigen los siguientes convenios para la creación de un bloque global de reglas de Firewall así como para la asignación a un módulo:

- Vista en la Security Configuration Tool

  Las reglas de Firewall globales sólo se pueden crear en el ajuste del Advanced Mode.

- Prioridad

  Reglas definidas localmente tienen, como estándar, una mayor prioridad que las reglas globales; por ello, nuevas reglas globales asignadas se agregan primero al final de la lista de reglas locales.

  La prioridad se puede modificar cambiando el emplazamiento en la lista de reglas.

- Granularidad

  Las reglas de Firewall globales sólo se pueden asignar a un módulo como bloque de reglas completo.

- Entras, modificar o eliminar reglas

  Las reglas de Firewall globales no se pueden editar en la lista de reglas de Firewall locales de las propiedades del módulo. Allí sólo se pueden ver y emplazar según la prioridad deseada

  No es posible eliminar una sola regla de un bloque de reglas asignado. Sólo se puede eliminar de la lista de reglas locales el bloque de reglas completo; con esto no se altera la definición en la lista de reglas globales.

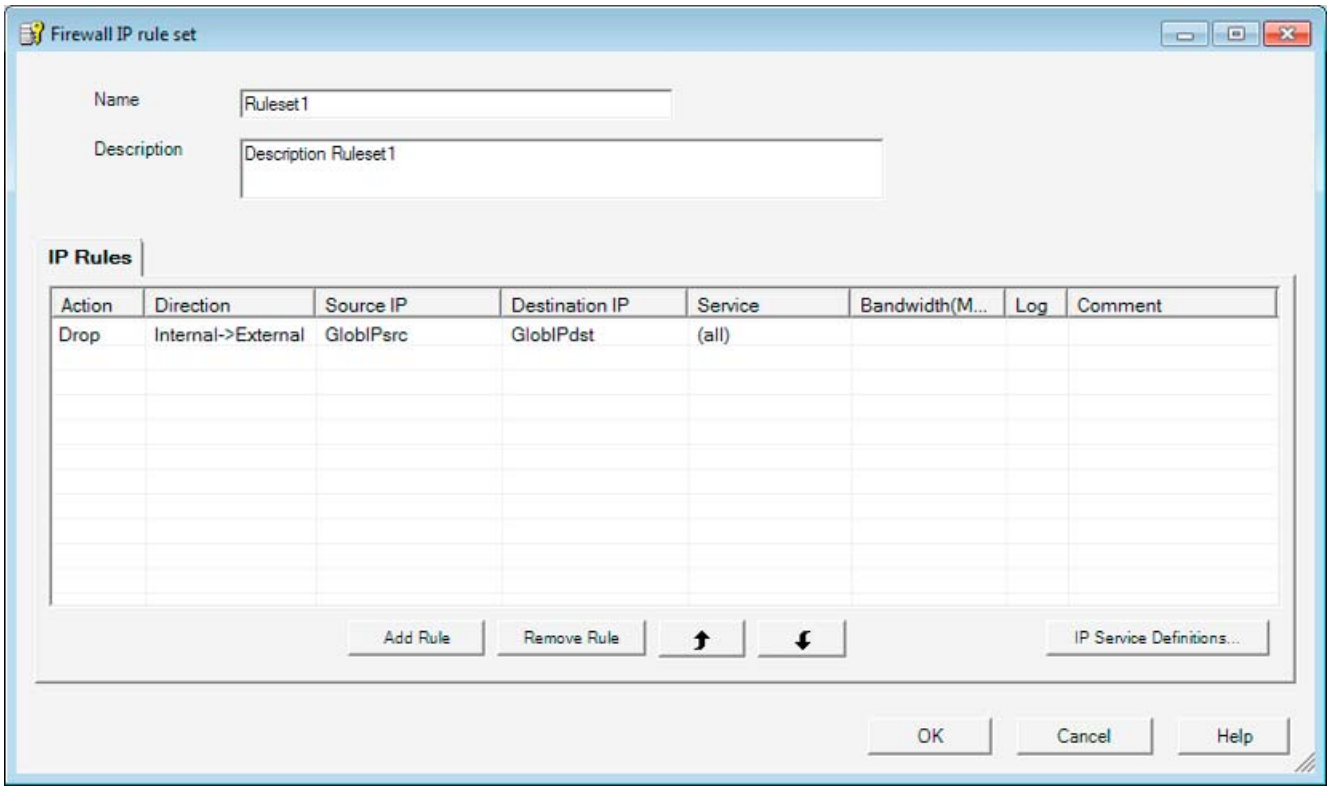
Ajustar y asignar reglas globales de filtros de paquetes

Si desea definir y asignar un bloque de reglas globales de Firewall, proceda del siguiente modo:

1. Seleccione una de las siguientes carpetas en el área de navegación:
   – Global FW-Rulesets / FW IP-Rulesets.
   – Global FW-Rulesets / FW MAC-Rulesets.
2. Seleccione el siguiente comando de menú para lcrear un bloque de reglas global:

   Insert ▸ Firewall rule set

3. Introduzca correlativamente las reglas de firewall en la lista; observe la siguiente descripción de parámetros y la evaluación en el capítulo siguiente o en la ayuda Online.
4. Asigne las reglas de Firewall globales a los módulos en las que se deban aplicar. Seleccione a tal fin un módulo en el área de navegación y arrástrelo al bloque de reglas globales adecuado en el área de navegación ("Drag and Drop").



Resultado:
el bloque de reglas globales es utilizado como bloque de reglas locales por el módulo asignado.

5.4.3 Ajuste de reglas de filtros de paquetes IP locales

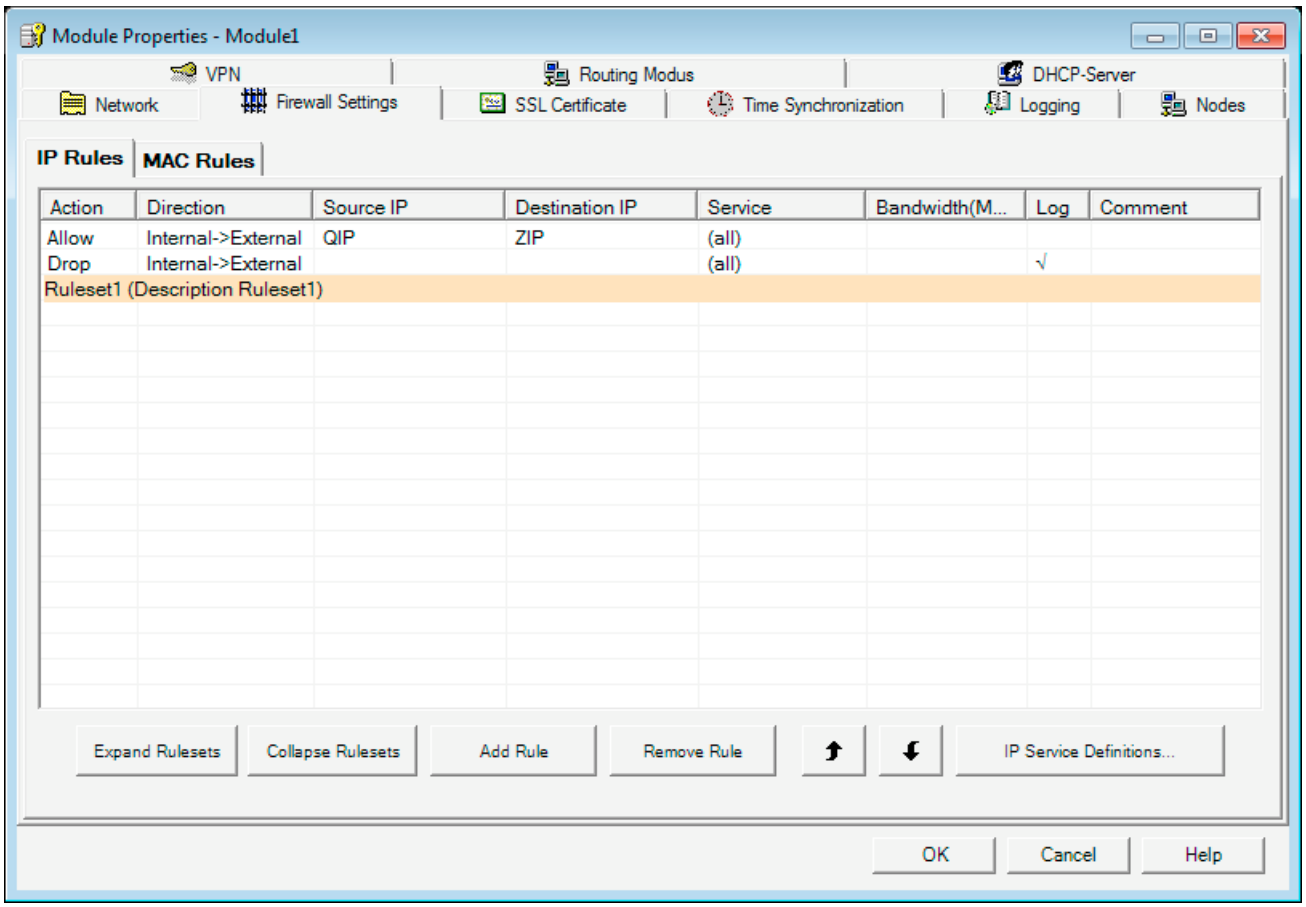
Por medio de reglas de filtrado de paquetes IP se pueden filtrar telegramas IP como por ejemplo telegramas UDP, TCP, ICMP.

Dentro de una regla de filtro de paquetes IP puede recurrir a definiciones de servicios para así delimitar aún más los criterios de filtrado. Si no indica ningún servicio, la regla de paquetes IP es válida para todos los servicios.

Abrir el cuadro de diálogo para reglas locales de filtrado de paquetes IP

Marque el módulo a editar y seleccione el siguiente comando de menú para configurar el firewall:

Edit ▸ Properties...



Registrar reglas de filtrado de paquetes IP

Introduzca correlativamente las reglas de firewall en la lista; observe la siguiente descripción de parámetros y los ejemplos en el capítulo siguiente o en la ayuda Online.

Uso de bloques de reglas globales

Los bloques de reglas globales asignados al módulo se adoptan automáticamente en el bloque de reglas locales. En un principio se encuentran al final de la lista, por lo que se tratan con la prioridad más baja. Puede modificar la prioridad cambiando de posición un bloque de reglas locales o globales en la lista de reglas.

La ayuda online le explica el significado de los distintos botones.

5.4.4 Reglas de filtrado de paquetes IP

Las reglas de filtrado de paquetes IP se editan según las siguientes evaluaciones:

- Parámetros registrados en la regla;
- Orden y la correspondiente prioridad de las reglas dentro del bloque de reglas.

Parámetros

La configuración de una regla IP contiene los siguientes parámetros:

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Action	Definición de la autorización (habilitación/bloqueo)	• Allow Autorizar telegramas según definición. • Drop Bloquear telegramas según definición.
Direction	Indica la dirección del tráfico de datos ("Tunnel / Any" sólo en S612 / S613)	• Internal → External • Internal ← External • Tunnel → Internal • Tunnel ← Internal • Internal → Any • Internal ← Any
Source IP	Dirección IP de origen	Véase el apartado "Direcciones IP en reglas de filtrado de paquetes IP" en este capítulo. Como alternativa puede introducir un nombre simbólico.
Destination IP	Dirección IP de destino	
Service	Nombre del servicio IP/ICMP o del grupo de servicios utilizado. Con ayuda de definiciones de servicios se pueden definir reglas de filtrado de forma compacta y clara Seleccione aquí uno de los servicios definidos por usted en el cuadro de diálogo para servicios IP: • Servicios IP o • Servicios ICMP Si no ha definido aún ningún servicio o si desea definir otro servicio, pulse el botón "IP/MAC Service Definitions..".	La lista desplegable le ofrece los servicios y grupos de servicios configurados, para su selección. Ninguna indicación significa: no se comprueba ningún servicio, la regla es válida para todos los servicios.
Bandwidth (Mbit/s)	Posibilidad de ajuste de una limitación del ancho de banda. Un paquete pasa el firewall si la regla de paso es correcta y si no se ha sobrepasado aún el ancho de banda permitido para esa regla.	Campo de valores: 0.001...100 MBit/s
Logging	Activación o desactivación del Logging para esta regla	
Comentario	Espacio para explicación propia de la regla	

Direcciones IP en reglas de filtrado de paquetes IP

La dirección IP consta de 4 números decimales en el campo de valores de 0 a 255, separados entre sí por un punto; ejemplo: 141.80.0.16

En la regla de filtrado de paquetes tiene las siguientes posibilidades de indicar direcciones IP:

- ninguna indicación

  No tiene lugar ninguna comprobación; la regla es válida para todas las direcciones IP.

- una dirección IP

  La regla es válida exactamente para la dirección indicada.

- Banda de direcciones

  La regla es válida para todas las direcciones IP incluidas en la banda de direcciones.

  Una banda de direcciones se define indicando la cantidad de posiciones de bits válidas en la dirección IP, a saber en la siguiente forma:

  [Dirección IP]/[Cantidad de bits a considerar]

  – [Dirección IP]/24 significa por consiguiente que sólo los 24 bits de valor más alto de la dirección IP se tienen en cuenta en la regla de filtrado; se trata de las tres primeras posiciones de la dirección IP.

  – [Dirección IP]/25 significa que sólo se tienen en cuenta en la regla de filtrado las tres primeras posiciones y el bit de valor más alto de la cuarta posición de la dirección IP.

Tabla 5- 3 Ejemplos de banda de direcciones IP

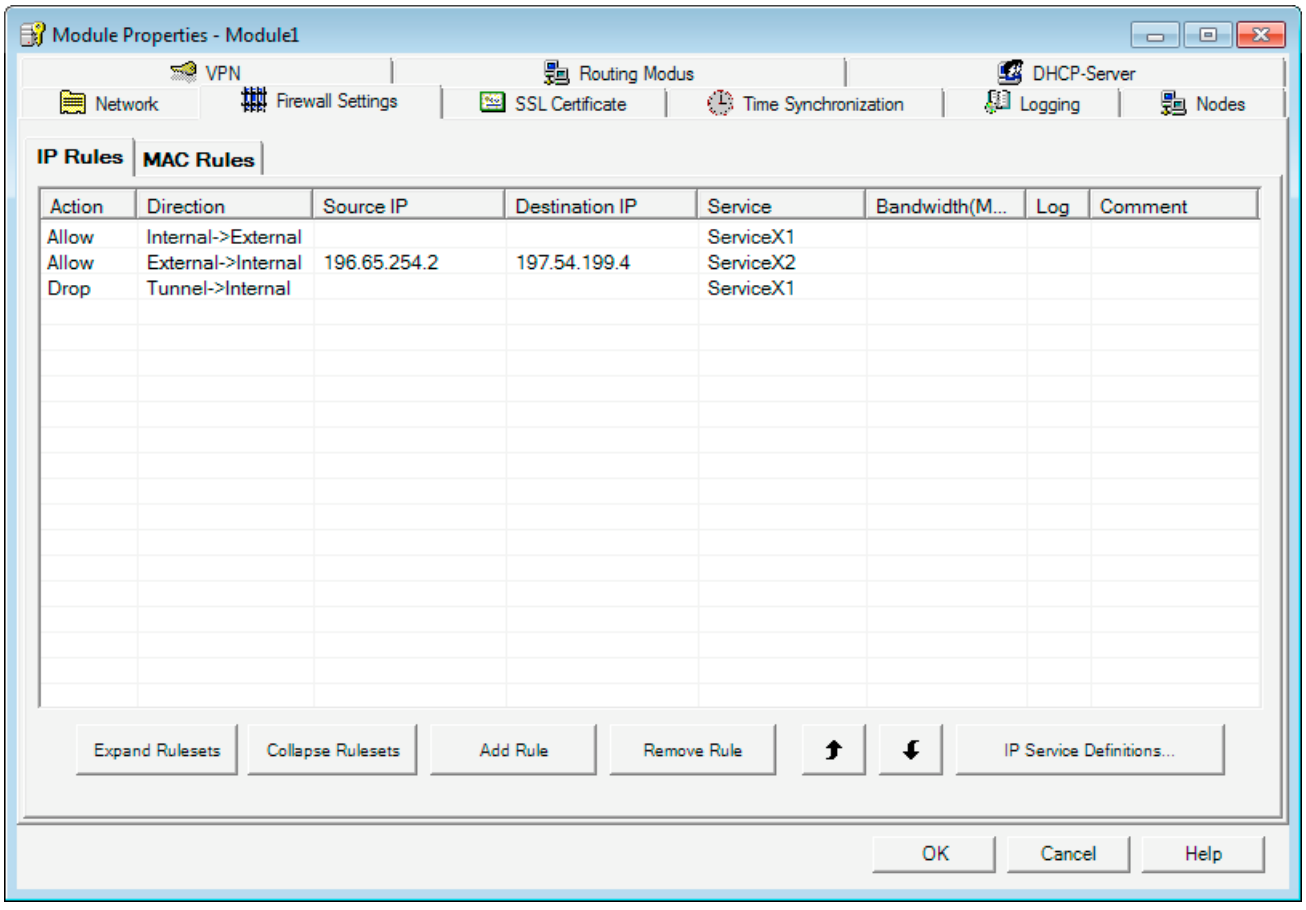
IP de origen o IP de destino	Banda de direcciones		Cantidad de direcciones *)
	de	a	
192.168.0.0/**16**	192.168.0.0	192.168.255.255	65.536
192.168.10.0/**24**	192.168.10.0	192.168.10.255	256
192.168.10.0/**25**	192.168.10.0	192.168.10.127	128
192.168.10.0/**26**	192.168.10.0	192.168.10.63	64
192.168.10.0/**27**	192.168.10.0	192.168.10.31	32
192.168.10.0/**28**	192.168.10.0	192.168.10.15	16
192.168.10.0/**29**	192.168.10.0	192.168.10.7	8
192.168.10.0/**30**	192.168.10.0	192.168.10.3	4
*) Nota: Tenga en cuenta que los valores de dirección 0 y 255 tienen una función especial en la dirección IP (0 representa una dirección de red, 255 representa una direección Broadcast). Con esto se reduce la cantidad de direcciones realmente disponibles.			

Orden de la evaluación de reglas por SCALANCE S

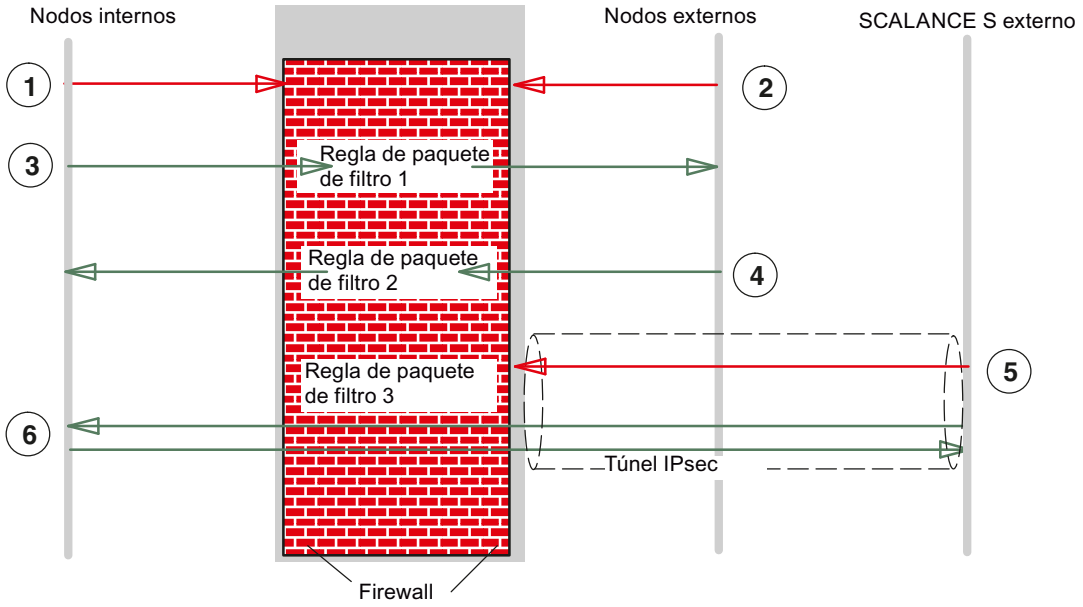
Las reglas de filtrado de paquetes son analizadas por SCALANCE S de la siguiente forma:

- La lista se analiza de arriba hacia abajo; en caso de reglas contradictorias vale por lo tanto siempre la entrada de más arriba.
- En el caso de reglas para comunicación entre la red interna y la externa, es válida la regla siguiente: están bloqueados todos los telegramas excepto los permitidos explícitamente en la lista.
- En el caso de reglas para comunicación entre red interna y túnel IPsec, es válida la regla siguiente: están permitidos todos los telegramas excepto los bloqueados explícitamente en la lista.

Ejemplo



Las reglas de filtrado de paquetes representadas a modo de ejemplo en el cuadro de diálogo anterior tienen como consecuencia el siguiente comportamiento:



① Todos los tipos de telegramas de interno hacia externo están bloqueados como estándar, excepto los permitidos explícitamente.

② Todos los tipos de telegramas de externo hacia interno están bloqueados como estándar, excepto los permitidos explícitamente.

③ La regla 1 de filtrado de paquetes IP permite telegramas con la definición de servicio "Service X1" de interno hacia externo.

④ La regla 2 de filtrado de paquetes IP permite telegramas de externo a interno si se cumple:

- Dirección IP del remitente: 196.65.254.2
- Dirección IP del destinatario: 197.54.199.4
- Definición de servicio: "Service X2"

⑤ La regla 3 de filtrado de paquetes IP bloquea telegramas con la definición de servicio "Service X2" en la VPN (túnel IPsec).

⑥ La comunicación por túnel IPsec está permitida como estándar, excepto para los tipos de telegramas bloqueados explícitamente.

5.4.5 Definir servicios IP

Con ayuda de definiciones de servicios IP se pueden definir de forma compacta y clara reglas de firewall que se aplican a diferentes servicios. Para esto se adjudica un nombre y se asignan al mismo los parámetros de servicio.

Además, los servicios así definidos se pueden reunir a su vez en grupos, con un nombre de grupo.

Para la configuración de las reglas de filtrado de paquetes globales o locales se utiliza entonces simplemente ese nombre.

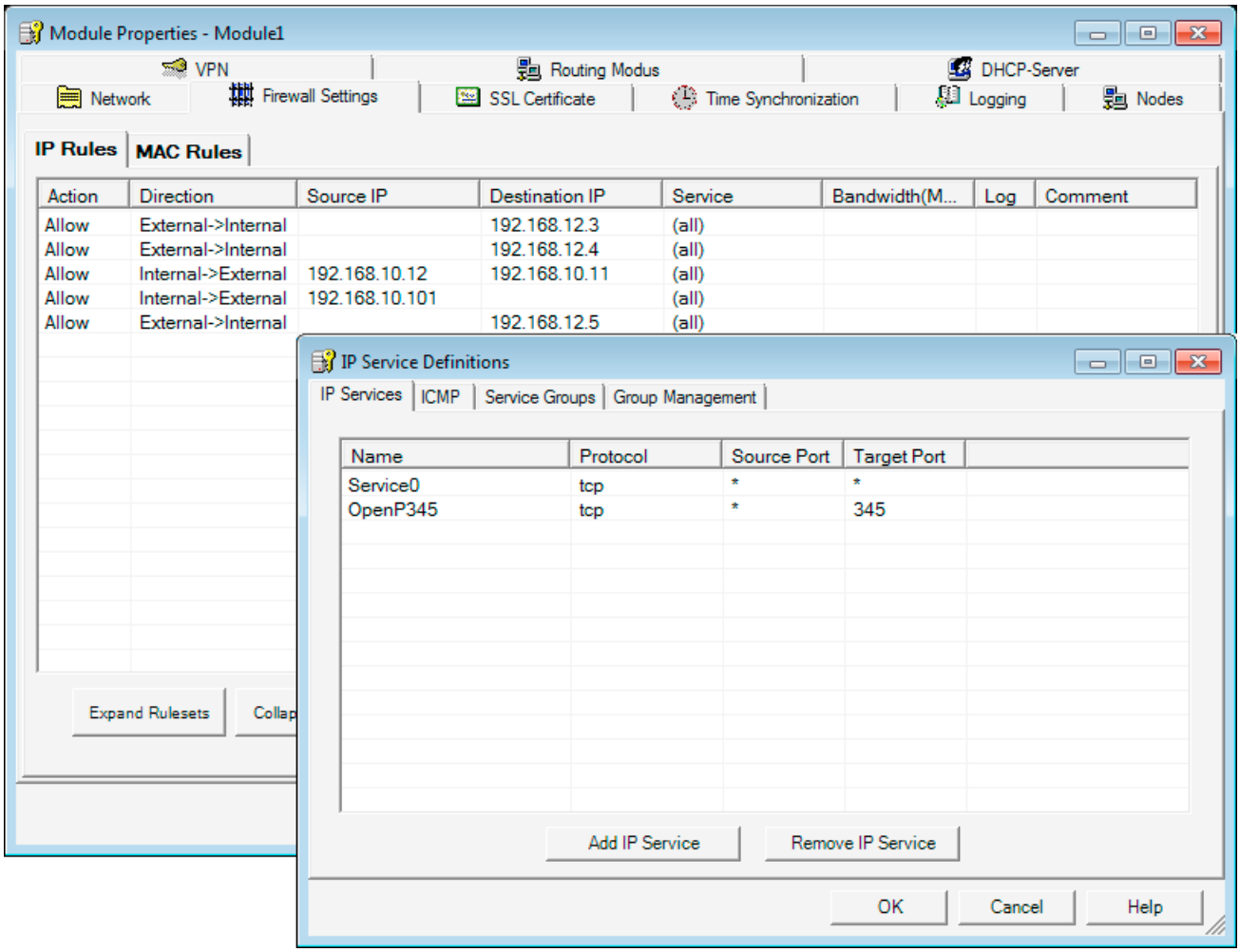
Cuadro de diálogo / ficha

Forma de abrir el cuadro de diálogo:

- Con el comando **Options ▸ IP/MAC Service Definitions...**

  o

- Desde la ficha "Firewall/IP Rules", con el botón "IP Service Definition...".



Parámetros para servicios IP

Los servicios IP se definen a través de los siguientes parámetros:

Tabla 5- 4 Servicios IP: Parámetros

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Name	Nombre de libre definición para el servicio; se utiliza para la identificación en la definición de reglas o en el agrupamiento.	Entrada libre
Protocol	Nombre del tipo de protocolo	TCP UDP Any (TCP y UDP)
Source Port	Tiene lugar un filtrado en base al número de puerto aquí indicado; éste define el acceso al servicio para el remitente de los telegramas.	Ejemplos: *: Puerto no se comprueba 20 ó 21: Servicio FTP
Target Port	Tiene lugar un filtrado en base al número de puerto aquí indicado; éste define el acceso al servicio para el destinatario de los telegramas.	Ejemplos: *: Puerto no se comprueba 80: Web-HTTP-Service 102: S7-Protocol - TCP/Port

5.4.6 Definir servicios ICMP

Con ayuda de definiciones de servicios ICMP se pueden definir de forma compacta y clara reglas de firewall que se aplican a diferentes servicios. Para esto se adjudica un nombre y se asignan al mismo los parámetros de servicio.

Además, los servicios así definidos se pueden reunir a su vez en grupos, con un nombre de grupo.

Para la configuración de las reglas de filtrado de paquetes se utiliza entonces simplemente ese nombre.

Cuadro de diálogo / ficha

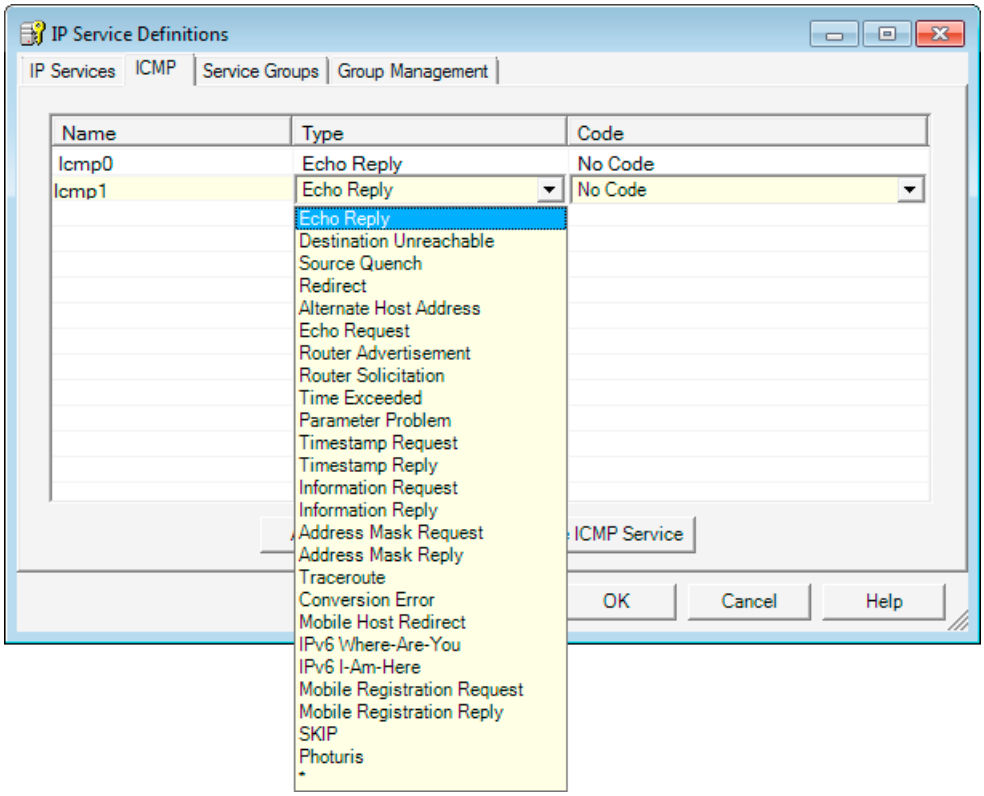
Forma de abrir el cuadro de diálogo:

- Sobre el comando de menú

  Options ▸ IP Service Definition...

  o

- Desde la ficha "Firewall", con el botón "IP Service Definition...".



Parámetros para servicios ICMP

Los servicios ICMP se definen a través de los siguientes parámetros:

Tabla 5- 5 Servicios ICMP: Parámetros

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Name	Nombre de libre definición para el servicio; se utiliza para la identificación en la definición de reglas o en el agrupamiento.	Entrada libre
Type	Tipo del mensaje ICMP	• ver representación del cuadro de diálogo
Code	Códigos del tipo ICMP	Los valores dependen del tipo seleccionado.

5.4.7 Ajustar reglas para filtrado de paquetes MAC

Por medio de reglas para filtrado de paquetes MAC se pueden filtrar telegramas MAC.

Nota

Routing Modus

Si ha activado el modo Routing para el módulo SCALANCE S, no tienen aplicación las reglas de MAC (los diálogos están inactivos).

Cuadro de diálogo / ficha

Marque el módulo a editar y seleccione el siguiente comando de menú para configurar el firewall:

Edit ▸ Properties..., ficha "Firewall", tabla "MAC Rules"

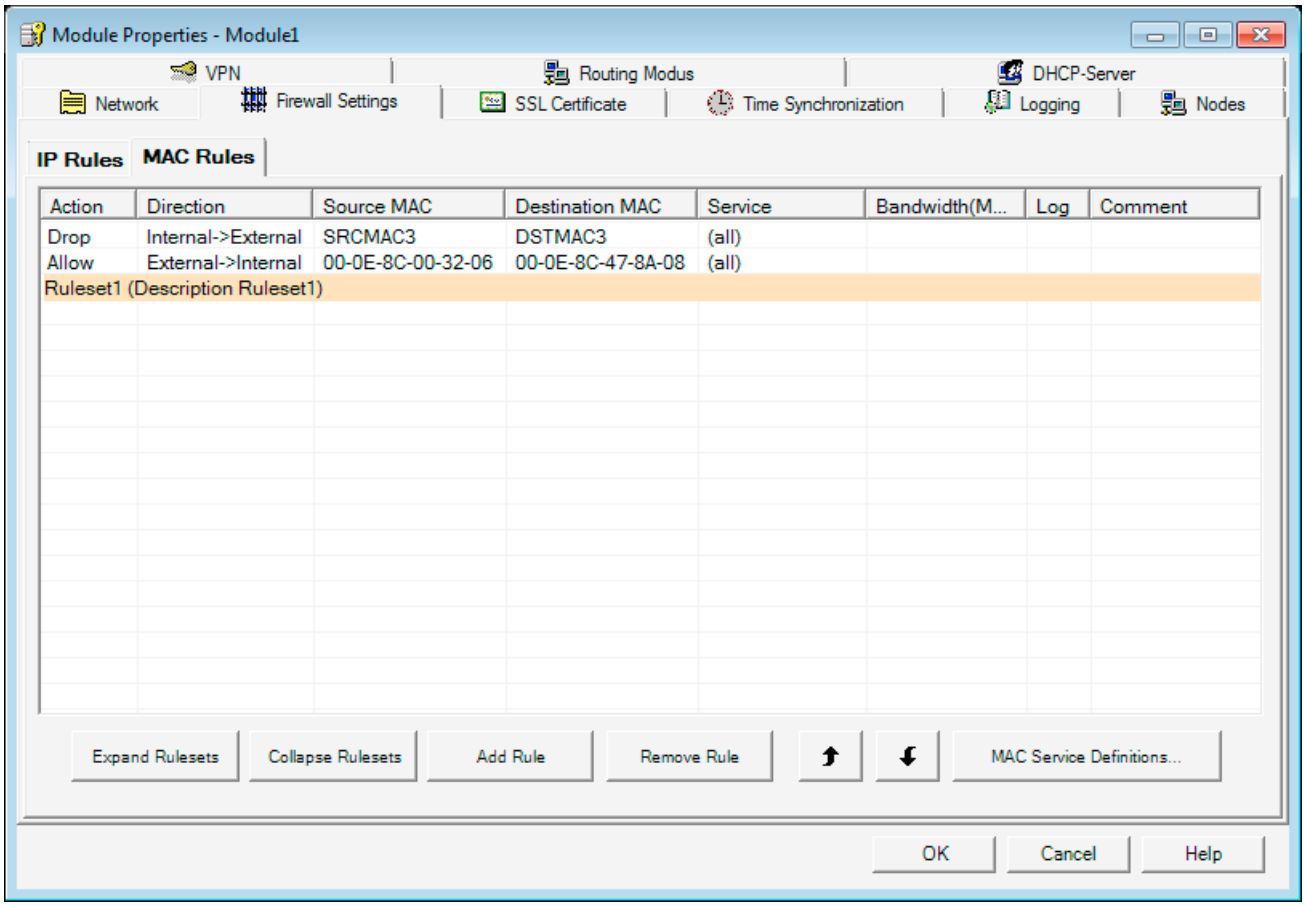


Figura 5-2 Diálogo "MAC Rules" en el ejemplo para SCALANCE S602

Introducir reglas de filtrado de paquetes

Introduzca correlativamente las reglas de firewall en la lista; observe la siguiente descripción de parámetros y los ejemplos en el capítulo siguiente o en la ayuda Online.

Uso de bloques de reglas globales

Los bloques de reglas globales asignados al módulo se adoptan automáticamente en el bloque de reglas locales. En un principio se encuentran al final de la lista, por lo que se tratan con la prioridad más baja. Puede modificar la prioridad cambiando de posición un bloque de reglas locales o globales en la lista de reglas.

La ayuda online le explica el significado de los distintos botones.

5.4.8 Reglas para filtrado de paquetes MAC

Las reglas de filtrado de paquetes MAC se editan según las siguientes evaluaciones:

- Parámetros registrados en la regla;
- Prioridad de las reglas dentro del bloque de reglas.

Reglas para filtrado de paquetes MAC

La configuración de una regla MAC contiene los siguientes parámetros:

Tabla 5- 6 Reglas MAC: Parámetros

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Action	Definición de la autorización (habilitación/bloqueo)	• Allow Autorizar telegramas según definición. • Drop Bloquear telegramas según definición.
Direction	Indica la dirección y el tipo del tráfico de datos ("Tunnel / Any" sólo en S612 / S613)	• Internal → External • Internal ← External • Tunnel → Internal • Tunnel ← Internal • Internal → Any • Internal ← Any
Quelle MAC	Dirección MAC de origen	Como alternativa a una dirección MAC puede introducir un nombre simbólico.
Ziel MAC	Dirección MAC de destino	

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Service	Nombre del servicio MAC o del grupo de servicios utilizado.	La lista desplegable le ofrece los servicios y grupos de servicios configurados, para su selección. Ninguna indicación significa: no se comprueba ningún servicio, la regla es válida para todos los servicios.
Bandwidth (Mbit/s)	Posibilidad de ajuste de una limitación del ancho de banda. Un paquete pasa el firewall si la regla de paso es correcta y si no se ha sobrepasado aún el ancho de banda permitido para esa regla.	Campo de valores: 0.001...100 MBit/s
Logging	Activación o desactivación del Logging para esta regla	
Comentario	Espacio para explicación propia de la regla	

Evaluación de reglas por SCALANCE S

Las reglas de filtrado de paquetes son analizadas por SCALANCE S de la siguiente forma:

- La lista se analiza de arriba hacia abajo; en caso de reglas contradictorias vale por lo tanto siempre la entrada de más arriba.
- En el caso de reglas para comunicación en dirección internal->external e internal<-external, rige para todos los telegramas registrados en forma no explícita: están bloqueados todos los telegramas excepto los permitidos explícitamente en la lista.
- En el caso d ereglas para comunicación en dirección internal->IPsec-Tunnel e internal<-IPsec-Tunnel, rige para todos los telegramas registrados en forma no explícita: están permitidos todos los telegramas excepto los bloqueados explícitamente en la lista.

ATENCIÓN
En el modo Bridge: Las reglas de IP sirven para paquetes de IP, las reglas MAC sirven para paquetes de nivel 2 (Layer-2) Si un módulo está en el modo Bridge, para el Firewall se pueden definir tanto reglas IP como reglas MAC. La edición en el Firewall se regula con el tipo de ethernet del paquete. Los paquetes IP se redirigen o se bloquean dependiendo de las reglas de IP, y los paquetes de nivel 2 (Layer 2) se redirigen o se bloquean dependiendo de las reglas MAC. No es posible filtra run paquete IP con la ayuda de una regla de firewall o cortafuegos MAC, por rejemplo, en lo que se refiere a una dirección MAC.

Ejemplos

El ejemplo del filtro de paquetes IP del capítulo 5.4.3 se puede utilizar por analogía para las reglas de filtrado de paquetes MAC.

5.4.9 Definir servicios MAC

Con ayuda de definiciones de servicios MAC se pueden definir de forma compacta y clara reglas de firewall que se aplican a diferentes servicios. Para esto se adjudica un nombre y se asignan al mismo los parámetros de servicio.

Además, los servicios así definidos se pueden reunir a su vez en grupos, con un nombre de grupo.

Para la configuración de las reglas de filtrado de paquetes globales o locales se utiliza entonces simplemente ese nombre.

Cuadro de diálogo

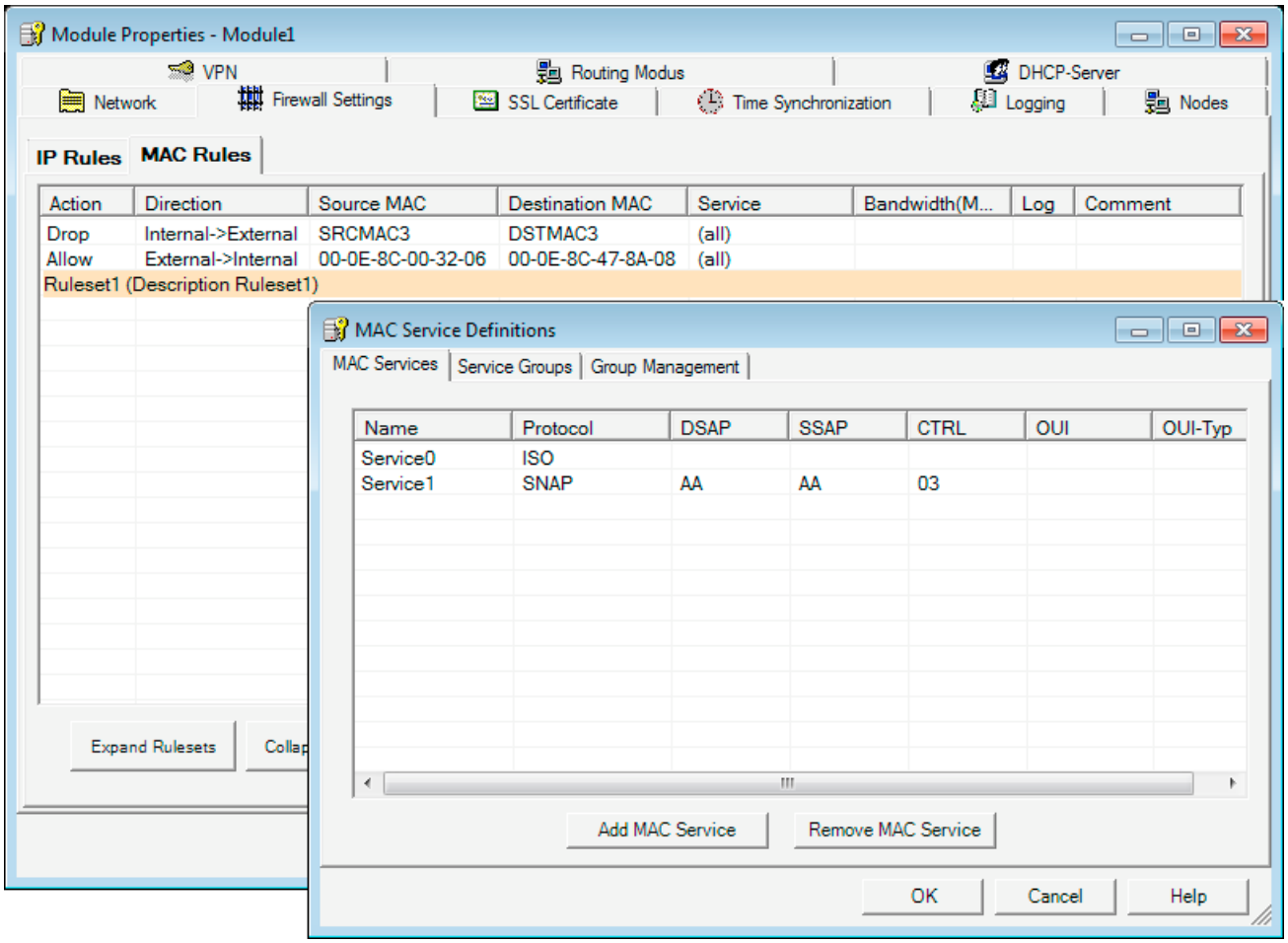
Forma de abrir el cuadro de diálogo:

- Sobre el siguiente comando de menú:

  Options ▸ MAC Service Definition...

  o

- Desde la ficha "Firewall/MAC Rules", con el botón "MAC Service Definition...".



Parámetros para servicios MAC

Una definición de servicio MAC contiene una categoría de parámetros MAC específicos del protocolo:

Tabla 5- 7 Parámetros de servicios MAC

Denominación	Significado/comentario	Posibilidades de selección / campos de valores
Name	Nombre de libre definición para el servicio; se utiliza para la identificación en la definición de reglas o en el agrupamiento.	Entrada libre
Protocol	Nombre del tipo de protocolo: • ISO ISO designa telegramas con las siguientes propiedades: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined • SNAP SNAP designa telegramas con las siguientes propiedades: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined	• ISO • SNAP • 0x (entrada de código)
DSAP	Destination Service Access Point: Dirección de destinatario LLC	
SSAP	Source Service Access Point: Dirección de remitente LLC	
CTRL	LLC Control Field	
OUI	Organizationally Unique Identifier (los 3 primeros bytes de la dirección MAC = identificación del fabricante)	
OUI-Type	Tipo de protocolo/identificación	
*) Las entradas de protocolo 0800 (hex) y 0806 (hex) no se aceptan, ya que estos valores corresponden a telegramas IP o ICMP. Estos telegramas se filtran mediante las reglas IP.		

Ajustes especiales para servicios SIMATIC NET

Utilice para el filtrado de servicios especiales SIMATIC NET los siguientes ajustes de SNAP:

- DCP (Primary Setup Tool) :

  PROFINET
- SiClock :

  OUI= 08 00 06 (hex) , OUI-Type= 01 00 (hex)

5.4.10 Configurar grupos de servicios

Formación de grupos de servicios

Varios servicios se pueden reunir formando grupos de servicios. De este modo se pueden crear servicios más complejos que entonces se pueden utilizar en las reglas de filtrado de paquetes seleccionando simplemente un nombre.

Cuadro de diálogo / ficha

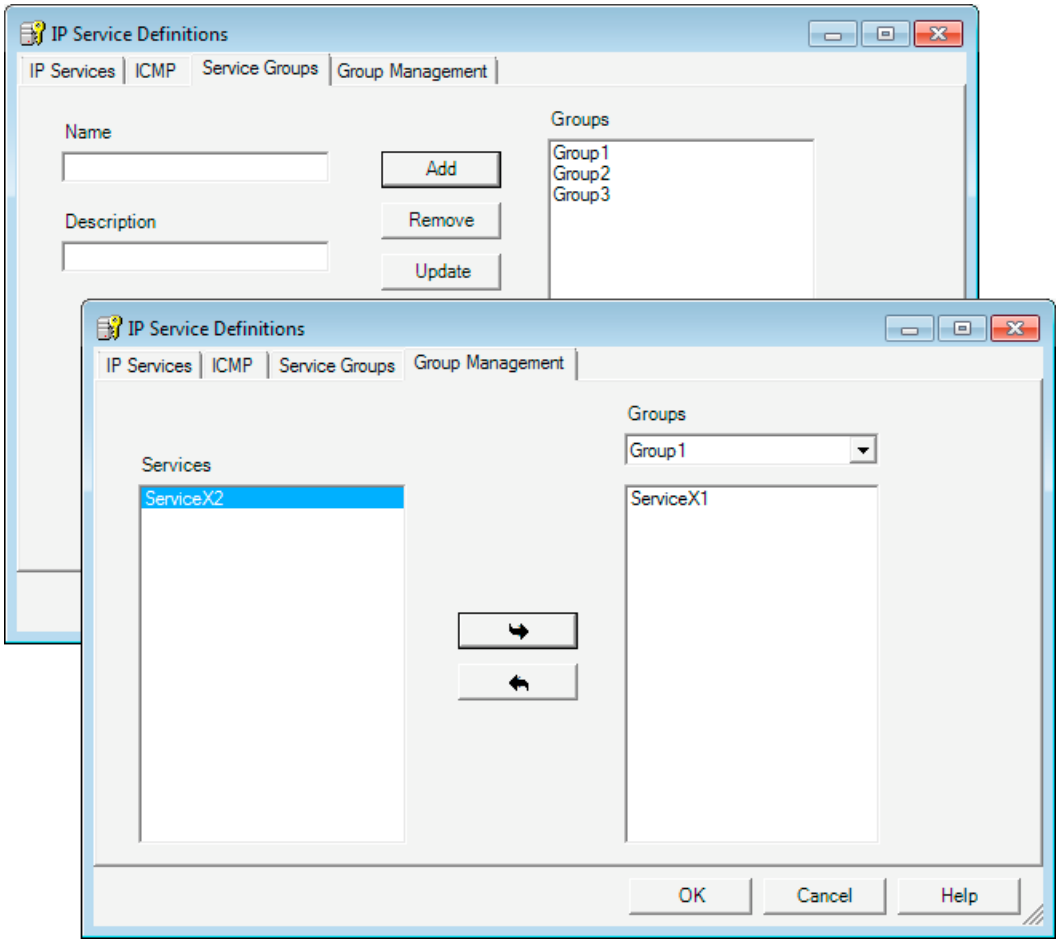
Forma de abrir el cuadro de diálogo:

- Sobre el siguiente comando de menú:

  Options ▸ IP/MAC Service Definition...

  o

- Desde la ficha "Firewall/IP Rules" o "Firewall/MAC Rules", con el botón "IP/MAC Service Definition.."



5.5 Sincronización horaria

Significado

Para comprobar la validez horaria de un certificado y para el sello horario de registros Log se indican la fecha y la hora en el módulo SCALANCE S.

Nota

La sincronización de tiempo se refiere únicamente al módulo SCALANCE S y no puede utilizarse para la sincronización de equipos en la red interna del SCALANCE S.

Alternativas de gestión de la hora

Se pueden configurar las siguientes alternativas:

- Hora local del PC

  La hora del módulo se ajusta automáticamente a la hora del PC al cargar una configuración.

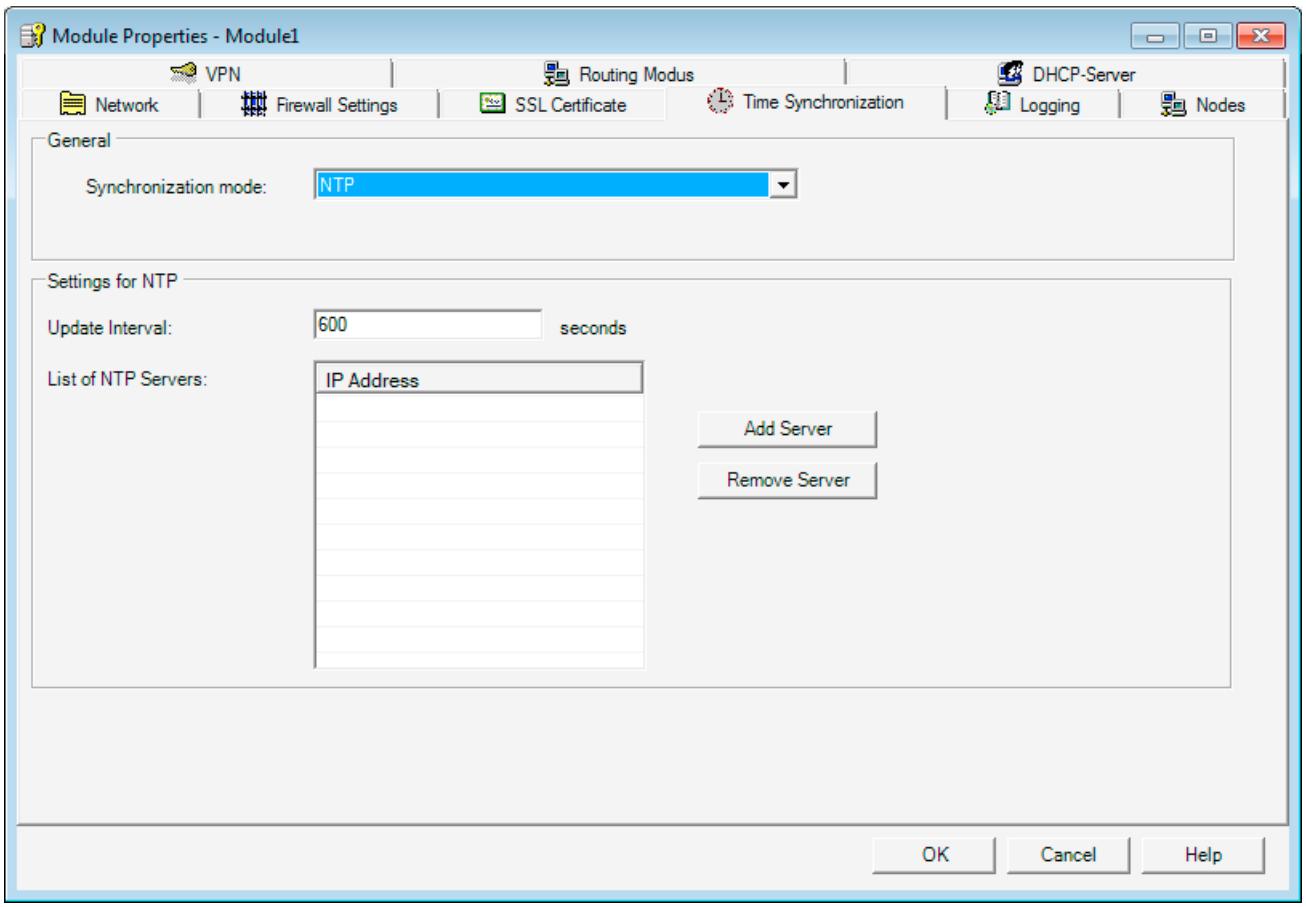
- Servidor NTP

  Ajuste automático y sincronización periódica de la hora a través de un servidor NTP (Network Time Protocol).

Abrir el cuadro de diálogo para configuración de la sincronización horaria

Marque el módulo a editar y seleccione el siguiente comando de menú:

Edit ▸ Properties..., ficha "Time synchronization"



Sincronización por un servidor de hora NTP

En caso de sincronización por medio de un servidor de hora NTP, al configurar tiene que indicar los siguientes dos parámetros:

- Dirección IP del servidor NTP
- el intervalo de actualización en segundos

ATENCIÓN
Si no es posible acceder al servidor NTP desde el Scalance S a través de una conexión túnel IPsec, los telegramas del servidor NTP se tienen que autorizar explícitamente en el firewall (UDP, Port 123).

Telegramas horarios externos

Los telegramas horarios externos no están asegurados y pueden ser falseados en la red externa. Esto puede ser causa, por ejemplo, de que la hora local sea comprometida en la red interna y en los módulos SCALANCE S.

Por esta razón, el servidor NTP se debería emplazar, a ser posible, en redes internas.

5.6 Creación de certificados SSL

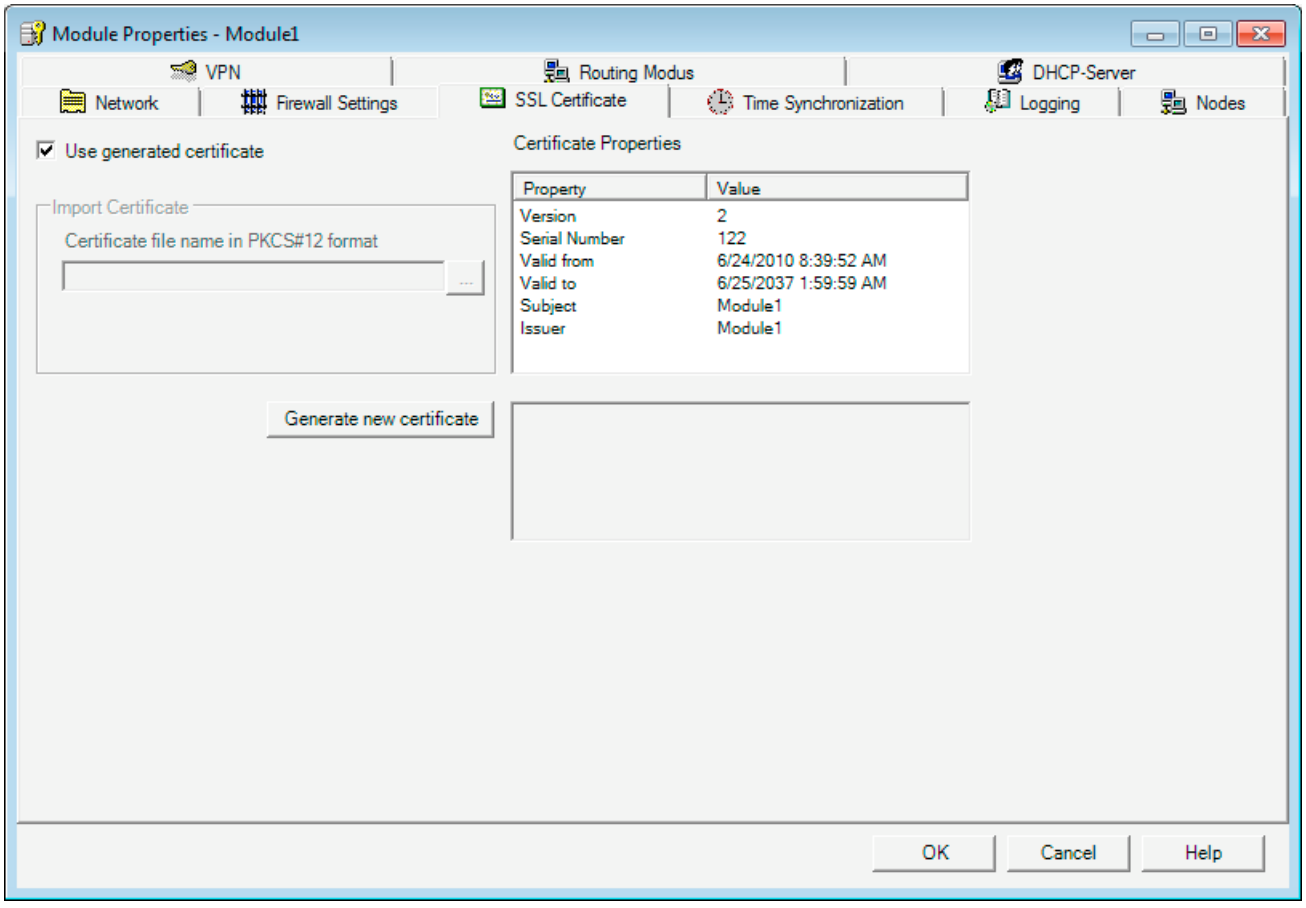
Significado

Los certificados SSL se utilizan para la autenticación de la comunicación entre un equipo y SCALANCE S para la comunicación en línea.

Abrir el cuadro de diálogo para administración de certificados SSL

Marque el módulo a editar y seleccione el siguiente comando de menú:

Edit ▸ Properties..., ficha "SSL certificates"



5.7 Routing Modus

5.7.1 Routing

Significado

Si ha activado el modo Routing, se transmiten los telegramas dirigidos a una dirección IP existente en la respectiva subred (interna o externa). Por lo demás son válidas las reglas de Firewall adoptadas para el respectivo sentido de transmisión.

Para este modo de operación tiene que configurar, en el cuadro de diálogo mostrado a continuación, una dirección IP interna y una máscara de subred interna para el direccionamiento del router en la subred interna.

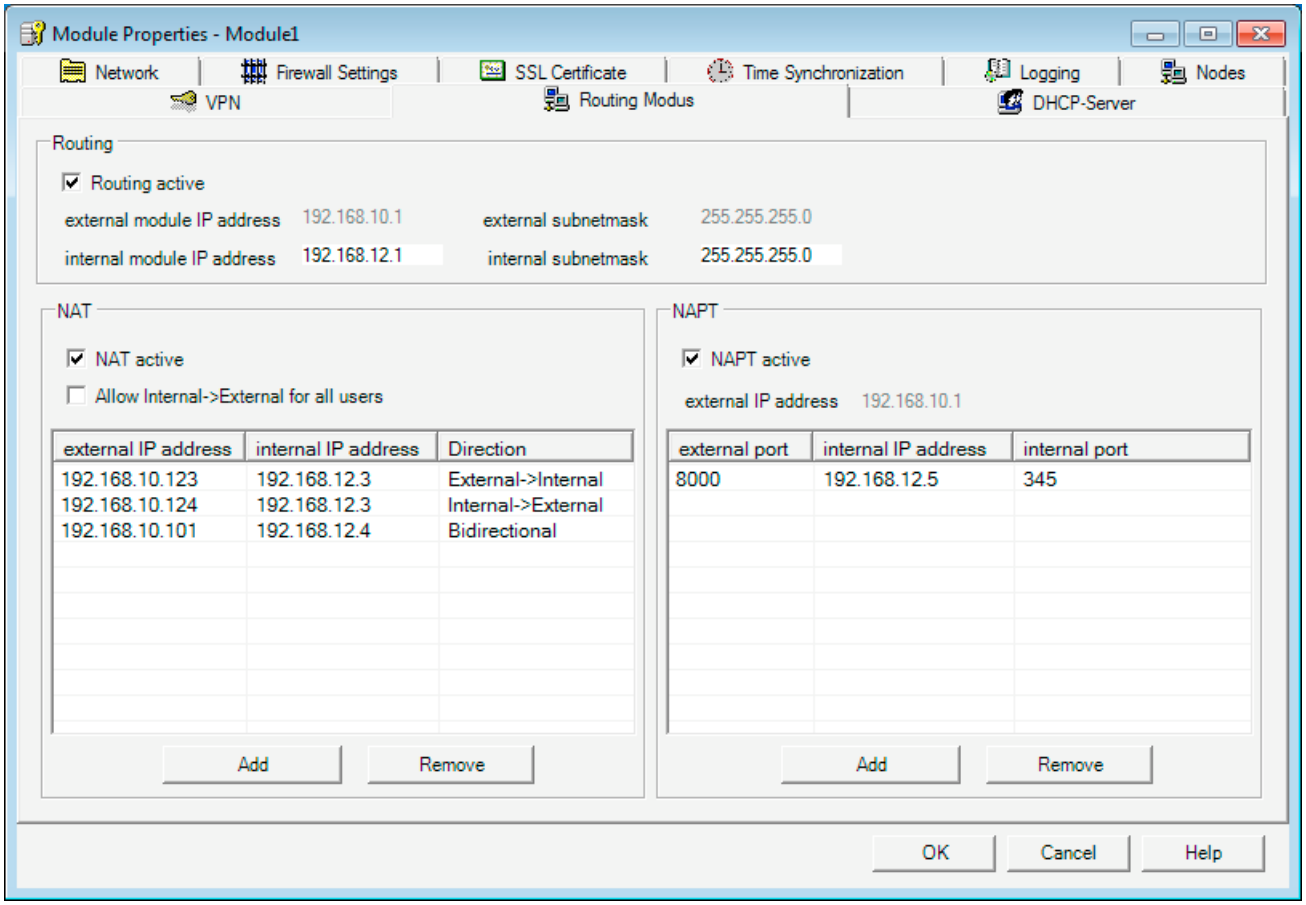
Vista de operación

Esta función se puede configurar de forma idéntica en Standard Mode y Advanced Mode.

Activar el modo Router

1. Marque el módulo a editar y seleccione el siguiente comando de menú:

Edit ▸ Properties..., ficha "Routing mode"



2. Seleccione la opción de Routing "activo".
3. Introduzca en los campos de entrada ahora activos una dirección IP interna y una máscara de subred interna para el direccionamiento del router en la subred interna.

5.7.2 Routing NAT/NAPT

Significado

Al configurar en el cuadro de diáologo "Routing Mode" una conversión (traducción) de direcciones, utiliza el SCALANCE S como router NAT/NAPT. Con esta técnica consigue que las direcciones de las estaciones de la subred no se den a conocer hacia el exterior en la red externa; las estaciones internas sólo se ven en la red externa a través de las direcciones IP externas definidas en la lista de conversión de direcciones (tabla NAT y tabla NAPT), estando así protegidas de acceso directo.

- NAT: Network Adress Translation
- NAPT: Network Address Port Translation

Vista de operación

Esta función está disponible en el Advanced Mode.

Para todas las funciones descritas en este capítulo, conmute el modo de funcionamiento con el siguiente comando de menú:

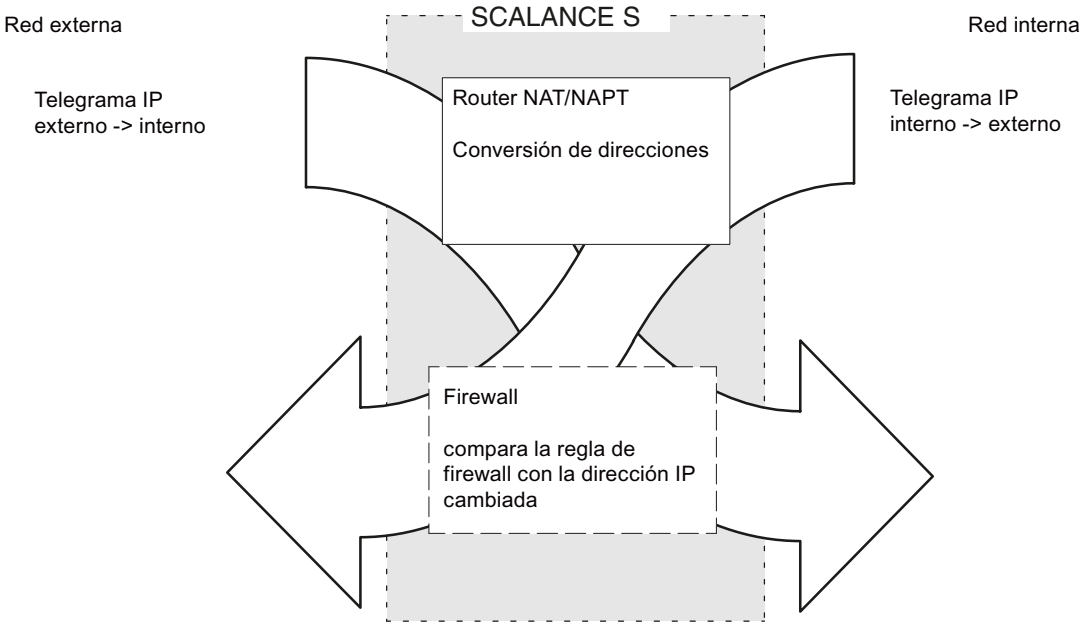
View ▸ Advanced Mode

El modo de operación aquí descrito incluye el uso como Standard Router. Tenga en cuenta por ello lo dicho en el capítulo "Routing".

Relación entre NAT/NAPT Router y Firewall

Para ambos sentido rige la regla de que los telegramas pasan primero por la conversión de direcciones en el NAT/NAPT Router y después por el Firewall. Los ajustes para el NAT/NAPT Router y las reglas de Firewall se tienen que adaptar entre sí de manera que telegramas con dirección convertida (traducida) puedan pasar el firewall.

Firewall y NAT/NAPT Router dan soporte al mecanismo "Stateful Packet Inspection". Por esta razón, los telegramas de respuesta pueden pasar el NAT/NAPT Router y el Firewall sin que sus direcciones se tengan que adoptar adicionalmente en las reglas de Firewall y en la conversión de direcciones de NAT/NAPT.



Observe los ejemplos de los capítulos siguientes.

Restricciones

En la lista aquí descrita tiene lugar una conversión de direcciones, definida estadísticamente, para las estaciones participantes en la red (subred) interna.

Edición del cuadro de diálogo para activación del NAT/NAPT Routing Mode

1. Marque el módulo a editar y seleccione el siguiente comando de menú:

   Edit ▸ Properties..., ficha "Routing mode"

2. Según se requiera, active una conversión de direcciones según NAT(Network Adress Translation) o NAPT (Network Address Port Translation).
3. Configure la conversión de direcciones según los siguientes datos.

Campo de entrada "NAT" (Network Adress Translation)

Aquí rige: Dirección = Dirección IP

Tabla 5- 8 Opciones NAT

Casillas de control	Significado
NAT active	Se activa el campo de entrada para NAT. Las conversiones de direcciones NAT sólo pasan a ser efectivas tras seleccionar la opción descrita a continuación y la inscripción en la lista de conversión de direcciones. Además tiene que configurar correspondientemente el firewall (vea los ejemplos).
Allow Internal > External for all users	Al seleccionar esta opción, se produce para todos los telegramas que van de interna a externa una conversión de la dirección IP interna en la dirección IP externa de módulo y un número de puerto asignado adicionalmente por el módulo. Este comportamiento se puede ver en la línea presentada adicionalmente en la parte inferior de la tabla NAT. El símbolo "*" que aparece allí en la columna "internal IP address" indica que se convierten todos los telegramas dirigidos de la red interna a la externa. Observación: Debido a este efecto en la lista de conversión de direcciones, esta opción está asignada al campo de entrada NAT a pesar de la asignación adicional de un número de puerto.

Tabla 5- 9 Tabla NAT

Parámetros	Significado/comentario	Posibilidades de selección / campos de valores
external IP address	• Para el sentido de telegramas "Internal → External": nueva dirección IP asignada • Para el sentido de telegramas "External → Internal": dirección IP reconocida	Véase el apartado "Direcciones IP en reglas de filtrado de paquetes IP" en este capítulo. Como alternativa puede introducir un nombre simbólico.
internal IP adress	• Para el sentido de telegramas "External → Internal": nueva dirección IP asignada • Para el sentido de telegramas "Internal → External": dirección IP reconocida	
Direction	Asigne aquí el sentido de transmisión de los telegramas. Efecto en el ejemplo "Internal → External": Telegramas procedentes de la subred interna se comprueban en cuanto a la dirección IP interna indicada y se transmiten a la red externa con la dirección IP externa indicada.	• Internal → External • external → internal • bidireccional

Campo de entrada "NAPT" (Network Address Port Translation)

Aquí rige: Dirección = Dirección IP + Número de puerto

Tabla 5- 10 Opciones NAPT

Casillas de control	Significado
NAPT active	Se activa el campo de entrada para NAPT. Las conversiones de direcciones NAPT sólo resultan efectivas tras la inscripción en la lista de conversión de direcciones. Además tiene que configurar correspondientemente el firewall (vea los ejemplos).
external IP address	Visualización de la dirección IP del módulo SCALANCE S utilizada como dirección de router por las estaciones participantes en la red externa.

Tabla 5- 11 Tabla NAPT

Parámetros	Significado/comentario	Posibilidades de selección / campos de valores
External port	Una estación de la red externa puede responder o enviar un telegrama a una estación de la subred interna utilizando el número de puerto de la misma.	Puerto o campo de puertos. Ejemplo de entrada de un campo de puertos: • 78:99
internal IP adress	Dirección IP de la estación aludida en la subred interna.	Véase el apartado "Direcciones IP en reglas de filtrado de paquetes IP" en este capítulo. Como alternativa puede introducir un nombre simbólico.
Internal port	Número de puerto de un servicio en la estación aludida en la subred interna.	Puerto (no campo de puertos)

Prueba de coherencia - reglas a considerar

Observe las reglas siguientes para la asignación de direcciones, con el fin de obtener entradas coherentes:

Prueba / Regla	Comprobación realizada	
	a nivel local	a nivel de proyecto
El ID de red de la subred interna tiene que ser diferente del ID de red de la subred externa.		x
Las direcciones IP internas no deben ser idénticas a las direcciones IP del módulo.		x
Adopte para el ID de red la parte determinada por la máscara de subred. • En el caso de la dirección IP externa, la parte de la dirección determinada por la máscara de subred externa se tiene que tomar de la dirección IP externa del SCALANCE S. • En el caso de la dirección IP interna, la parte de la dirección determinada por la máscara de subred interna se tiene que tomar de la dirección IP interna del SCALANCE S.		x
Una direcicón IP utilizada en la lista de conversión de direcciones NAT/NAPT no debe ser dirección Multicast ni dirección Broadcast.		x
El router predeterminado tiene que estar en una de las dos subredes del SCALANCE S, es decir, tiene que ser conforme a la dirección IP externa o a la interna.		x
Puertos externos asignados a la conversión NAPT han de estar en el campo > 0 y <= 65535. Quedan excluidos el Port123 (NTP), 443 (HTTPS), 514 (Syslog) y 500+4500 (IPsec; sólo para S612 y S613).	x	

Prueba / Regla	Comprobación realizada	
	a nivel local	a nivel de proyecto
La dirección IP externa del SCALANCE S sólo se debe utilizar en la tabla NAT para el sentido "Internal → External".	x	
La dirección IP interna del SCALANCE S no se debe utilizar en la tabla NAT ni en la tabla NAPT.		x
Control de duplicidad en la tabla NAT Una dirección IP externa utilizada con sentido "External → Internal" o "Bidireccional" sólo debe aparecer una vez en la tabla NAT.	x	
Control de duplicidad en la tabla NAPT • Un número de puerto externo sólo debe estar registrado una vez. Dado que siempre se utiliza la dirección IP de SCALANCE S como dirección IP externa, en caso de uso múltiple no tendría carácter inequívoco. • Los números de puerto o los campos de puertos externos no se deben superponer.	x	
En cuanto se activa el Routing Mode, se tienen que asignar al SCALANCE S las segundas direcciones (IP/subred).		x
Puertos NAPT internos pueden estar en el campo > 0 y <= 65535.	x	

Una vez finalizadas sus entradas, realice una prueba de coherencia.

Seleccione para ello el comando de menú:

Options ▸ Check Consistency

5.7.3 Routing NAT/NAPT - Ejemplos de configuración, parte 1

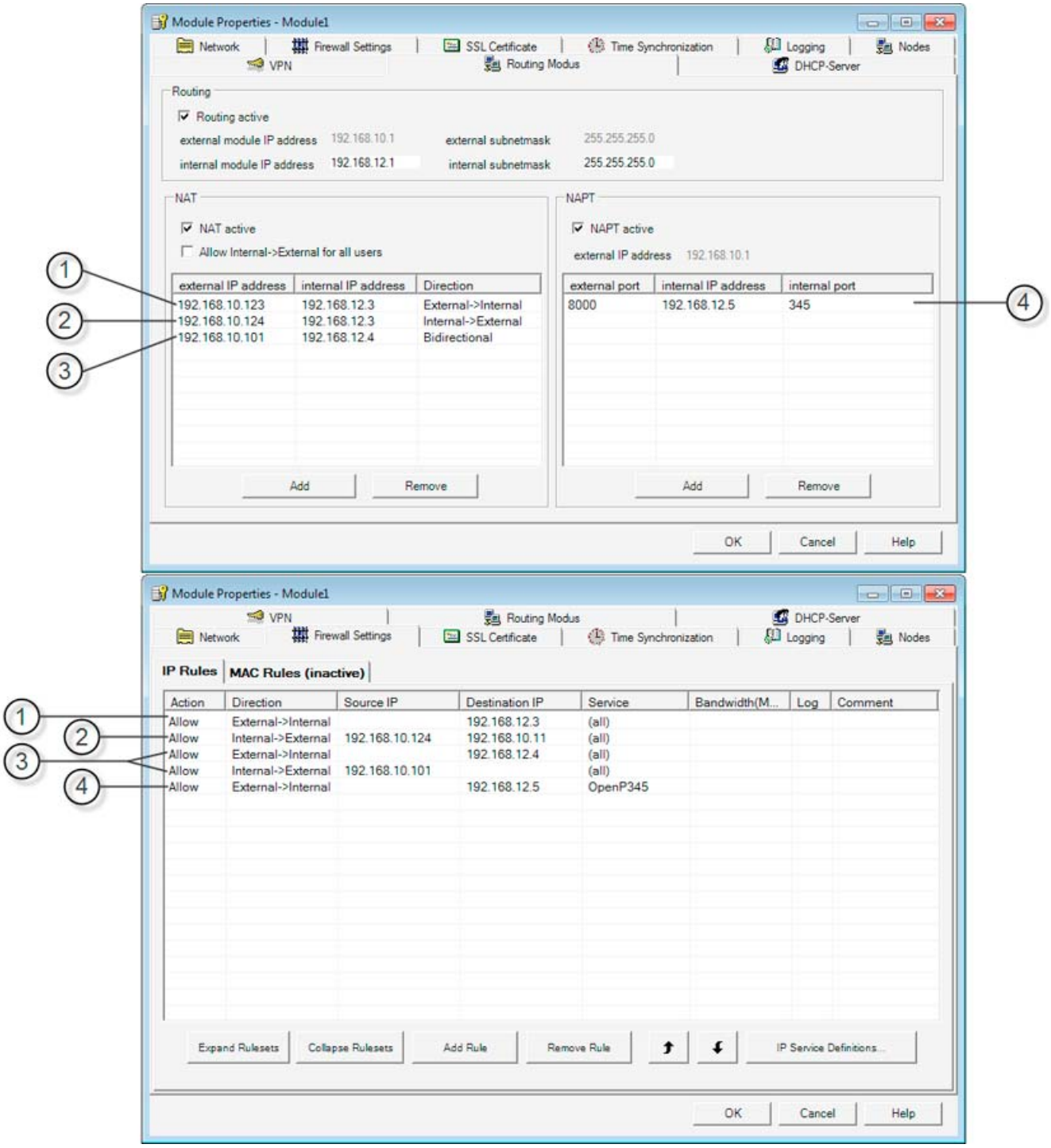
Resumen

En este capítulo encontrará los siguientes ejemplos de configuración del router NAT/NAPT:

- Ejemplo 1: Conversión de direcciones NAT "External → Internal"
- Ejemplo 2: Conversión de direcciones NAT "Internal → External"
- Ejemplo 3: Conversión de direcciones NAT "Bidirectional"
- Ejemplo 4: Conversión de direcciones NAPT

Configuración

En la siguiente configuración de routing encontrará asignaciones de direcciones según la conversión de direcciones NAT y NAPT:



Descripción

- **Ejemplo 1: Conversión de direcciones NAT "External → Internal"**

  Una estación de la red externa puede enviar un telegrama a la estación con la dirección IP interna 192.168.12.3 de la subred interna, utilizando la dirección IP externa 192.168.10.123 como dirección de destino.

- **Ejemplo 2: Conversión de direcciones NAT "Internal → External"**

  Telegramas de una estación interna con la dirección IP interna 192.168.12.3 son transmitidas a la red externa con la dirección IP externa 192.168.10.124 como dirección de origen. En el ejemplo, el firewall se ha configurado de manera que permita el paso de los telegramas con la dirección IP de origen 192.168.10.124 en el sentido de interna a externa, pudiendo alcanzar así la estación con la dirección IP 192.168.10.11.

- **Ejemplo 3: Conversión de direcciones NAT "Bidirectional"**

  En este ejemplo, la conversión de direcciones se efectúa en la foma descrita a continuación para telegramas entrantes tanto internos como externos:

  – Una estación de la red externa puede enviar un telegrama a la estación con la dirección IP interna 192.168.12.4 de la subred interna, utilizando la dirección IP externa 192.168.10.101 como dirección de destino.

  – Telegramas de una estación interna con la dirección IP interna 192.168.12.4 son transmitidas en la red externa con la dirección IP externa 192.168.10.101 como dirección de origen. El firewall se ha configurado de forma que permita el paso telegramas con la dirección IP de origen 192.168.10.101 en el sentido de interna a externa.

- **Ejemplo 4: Conversión de direcciones NAPT**

  Las conversiones de direcciones tienen lugar según NAPT, asignándose en cada caso adicionalmente números de puerto. Todos los telegramas TCP y UDP entrantes en la red externa son comprobados en cuanto a su dirección IP de destino y su número de puerto de destino.

  – Una estación de la red externa puede enviar un telegrama a la estación con la dirección IP interna 192.168.12.4 y el número de puerto 345 de la subred interna, utilizando como dirección de destino la dirección IP externa de módulo 192.168.10.1 y el número de puerto externo 8000.

5.7.4 Routing NAT/NAPT - Ejemplos de configuración, parte 2

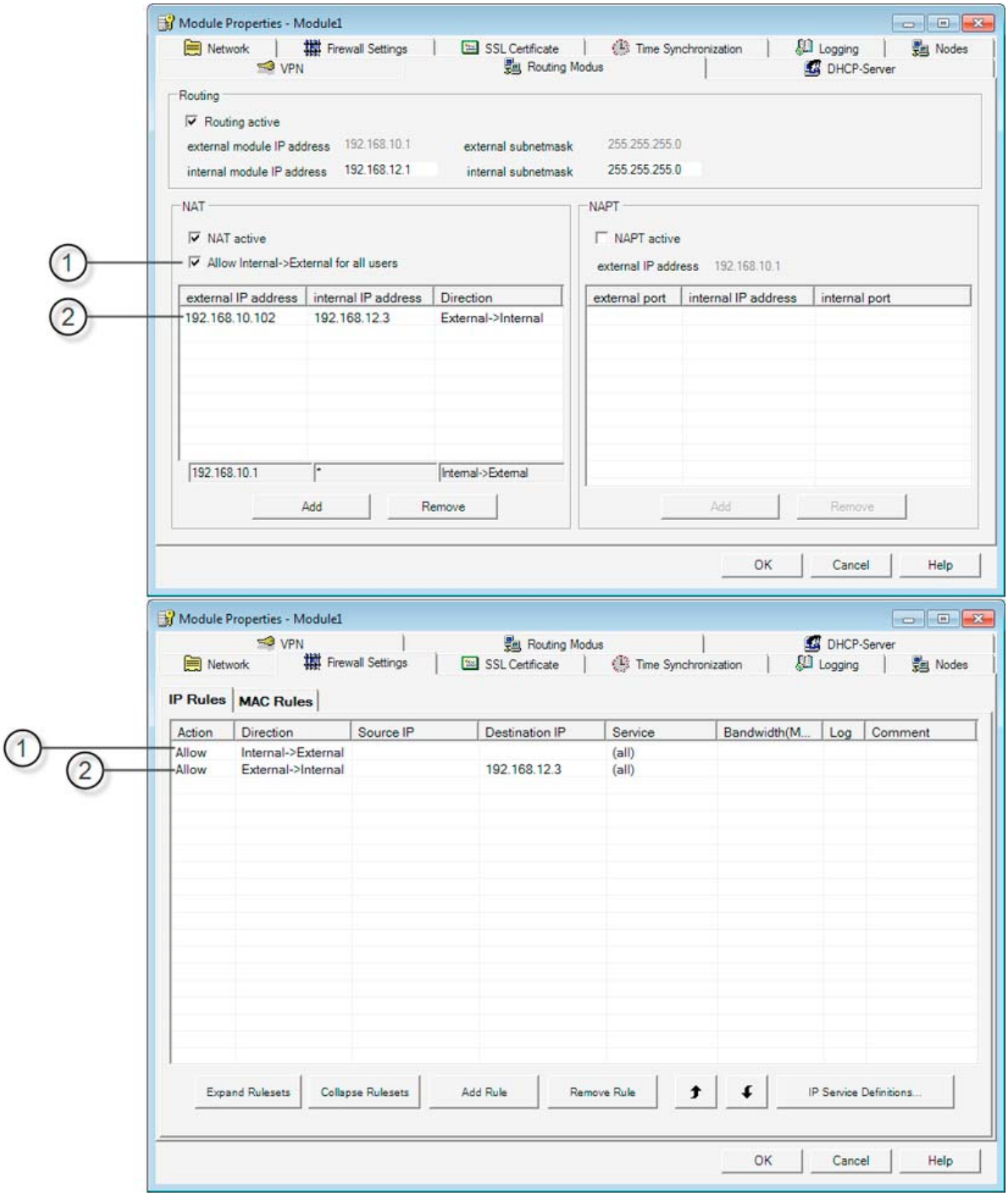
Resumen

En este capítulo encontrará los siguientes ejemplos de configuración del router NAT/NAPT:

- Ejemplo 1: Permitir todas las estaciones internas para comunicación externa
- Ejemplo 2: Permitir telegramas adicionales dirigidos de externa a interna.

Configuración

En la siguiente configuración de routing encontrará asignaciones de direcciones según la conversión de direcciones NAT:



Descripción

Ejemplo 1 - Permitir todas las estaciones internas para comunicación externa

En el campo de diálogo "NAT" está activada la casilla de control "Allow Internal -> External for all users".

Con esto es posible la comunicación de interna a externa. La conversión de direcciones tiene lugar así de forma que todas las direcciones internas se convierten en la dirección IP externa de SCALANCE S y un número de puerto asignado dinámicamente.

Ahora ya no es relevante la indicación de sentido en la lista de conversión de direcciones NAT. Todos los restantes datos se refieren al sentido de comunicación "externa hacia interna".

Además, el firewall está configurado de manera que puedan pasar los telegramas en el sentido de interna hacia externa.

Ejemplo 2 - Permitir telegramas adicionales dirigidos de externa a interna.

Para que, como complemento del ejemplo 1, se permita la comunicación de externa hacia interna, se han de introducir informaciones en la lista de conversión de direcciones NAT o NAPT. La entrada del ejemplo indica que telegramas dirigidos a las estaciones con la dirección IP 192.168.10.102 se convierten a la dirección IP interne 192.168.12.3.

El firewall se tiene que configurar correspondientemente. Dado que primero se produce siempre la conversión NAT/NAPT y sólo en un segundo paso se comprueba la direción convertida en el firewall, en el ejemplo la dirección IP interna está registrada en el firewall como dirección IP de destino.

5.8 Servidor DHCP

Resumen

Puede utilizar SCALANCE S como DHCP-Server en la red interna. Esto permite asignar automáticamente direcciones IP a los equipos conectados a la red interna.

Las direcciones se asignan en este caso dinámicamente, desde una banda de direcciones definida por usted, o bien se asigna una dirección IP a un equipo concreto conforme a sus predeterminaciones.

Conmmutar al Advanced Mode

La configuración como DHCP Server es posible en la vista "Advanced Mode" de la Security Configuration Tool. Conmute el modo de funcionamiento con el siguiente comando:

View ▸ Advanced Mode

Requisito

Tiene que configurar los equipos en la red interna de manera que obtengan la dirección IP de un servidor DHCP.

Dependiendo del modo de funcionamiento, el SCALANCE S transmite a las estaciones participantes en la subred una dirección IP de router, o bien se tiene que comunicar una dirección IP de router a las estaciones de la subred.

- Se transmite la dirección IP del router

  En los casos siguientes, el SCALANCE S transmite a las estaciones una dirección IP de router a través del protocolo DHCP:

  – SCALANCE S está configurado para el modo Router;

    SCALANCE S transmite en este caso la dirección IP propia como dirección IP del router

  – SCALANCE S no está configurado para el modo Router, pero en la configuración del SCALANCE S se ha indicado un router predeterminado (Default Router);

    SCALANCE S transmite en este caso la dirección IP del Default Router como dirección IP del router

- No se transmite la dirección IP del router

  En estos casos tiene que introducir manualmente la dirección IP del router en las estaciones:

  – SCALANCE S no está configurado para el modo Router;

  – En la configuración del SCALANCE S no se ha indicado Default Router.

Variantes

Para la configuración tiene las dos posibilidades siguientes:

- Asignación estática de direcciones

  A equipos con una dirección MAC o un Client-ID determinados se les asignan direcciones predeterminadas para cada caso. Introduzca para ello estos equipos en la lista de direcciones en el campo de entradas "Static IP addresses".

- Asignación dinámica de direcciones

  Equipos cuya dirección MAC o su Client-ID no se hayan indicado explícitamente reciben una dirección IP cualquiera de una banda de direcciones predeterminada. Esta banda de direcciones se ajusta en el campo de entrada "Dynamic IP addresses".

ATENCIÓN
Asignación dinámica de direcciones - Comportamiento tras una interrupción de la alimentación eléctrica Tenga en cuenta que las direcciones IP asignadas dinámicamente no se almacenan si se interrumpe la alimentación eléctrica. Tras restablecerse la alimentación eléctrica tiene que cuidar por tanto de que todas las estaciones soliciten de nuevo una dirección IP. Por esta razón, sólo debería prever la asignación dinámica de direcciones para las siguientes estaciones: • estaciones que se utilicen temporalmente en la subred (por ejemplo, equipos de mantenimiento); • estaciones que en caso de una nueva solicitud transmitan al DHCP Server como "dirección preferida" una dirección IP anteriormente asignada (por ejemplo, estaciones de PC). Para las estaciones que están en servicio permanente se debe preferir la asignación estática de direcciones indicando un Client-ID (esto se recomienda para CPs S7, por resultar más fácil la sustitución de módulos) o la dirección MAC.

Se da soporte a nombres simbólicos

En las función descrita a continuación puede introducir tanto direcciones IP o MAC como nombres simbólicos.

Prueba de coherencia - reglas a considerar

Al realizar sus entradas debe tener en cuanta las reglas indicadas a continuación.

Prueba / Regla	Prueba realizada [1]	
	a nivel local	a nivel de proyecto/módulo
Las direcciones IP asignadas en el campo de entradas "Static IP addresses" de la lista de direcciones no deben estar en el campo de direcciones IP dinámicas.		X
Los nombres simbólicos han de tener una asignación de dirección numérica. Si asigna aquí nuevos nombres simbólicos, tiene que realizar aún la asignación de direcciones en el cuadro de diálogo "Symbolic names".		X
Direcciones IP, direcciones MAC y Client-IDs sólo deben aparecer una vez en la tabla "Static IP addresses" (con referencia al módulo SCALANCE S).		X
En el caso de las direcciones IP asignadas estáticamente tiene que indicar la dirección MAC o el Client-ID (nombre del ordenador).	X	

Prueba / Regla	Prueba realizada [1]	
	a nivel local	a nivel de proyecto/módulo
El Client-ID es una secuencia de como máximo 63 caracteres. Sólo se permiten los caracteres siguientes: a-z, A-Z, 0-9 y - (guión). Nota: En el caso de SIMATIC S7 se puede asignar a los equipos conectados a la interfaz Ethernet un Client-ID para obtener una dirección IP a través de DHCP. En el caso de PCs, el procedimiento depende del sistema operativo utilizado; se recomienda utilizar en este caso la dirección MAC para la asignación.	X	
En el caso de las direcciones IP asignadas estáticamente, tiene que indicar la dirección IP.	X	
Las siguientes direcciones IP no deben estar en el área de la banda de direcciones IP libres (direcciones IP dinámicas): • todas las direcciones de router en la ficha "Network" • NTP-Server • Syslog-Server • Default-Router • Direcciones de SCALANCE S		X
DHCP es soportado por SCALANCE S en la interfaz con la subred interna. De este comportamiento operativo del SCALANCE S se derivan los siguientes requisitos para direcciones IP en el área de la banda de direcciones IP libres (direcciones IP dinámicas): • Uso en redes planas El área de la banda libre de direcciones IP tiene que estar en la red definida por SCALANCE S. • Modo Router El área de la banda libre de direcciones IP tiene que estar en la subred interna definida por SCALANCE S.		X
La banda libre de direcciones IP se tiene que indicar completa introduciendo la dirección IP inicial y la dirección IP final. La dirección IP final tiene que ser mayor que la dirección IP inicial.	X	
Las direcciones IP introducidas en la lista de direcciones en el campo de entrada "Static IP addresses" tiene que estar en el área de direcciones de la subred interna del módulo SCALANCE S.		X

Leyenda:

[1] Observe las explicaciones del capítulo "Pruebas de coherencia".

Comunicación segura en la VPN a través de túnel IPsec (S612/S613)

6

El tema tratado en este capítulo es cómo se unen por "arrastrar y colocar" las subredes IP protegidas por SCALANCE S para formar una Virtual Private Network.

Tal como se ha descrito ya en el capítulo 5 para las propiedades de los módulos, también aquí se pueden conservar los ajustes predeterminados para practicar una comunicación segura dentro de su red interna.

Otras informaciones

La ayuda online le proporcionará también información detallada sobre los diálogos y los parámetros ajustables.

Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

Consulte también

Funciones online - Test, Diagnóstico y Logging (Página 221)

6.1 VPN con SCALANCE S

Conexión segura a través de red no protegida

En las redes internas protegidas por SCALANCE S, los túneles IPsec proporcionan a los nodos una conexión de datos segura a través de la red externa no segura.

El intercambio de datos de los equipos a través de túnel IPsec en la VPN tiene con esto las siguientes propiedades:

- Confidencialidad

  Los datos intercambiados están protegidos de escuchas.

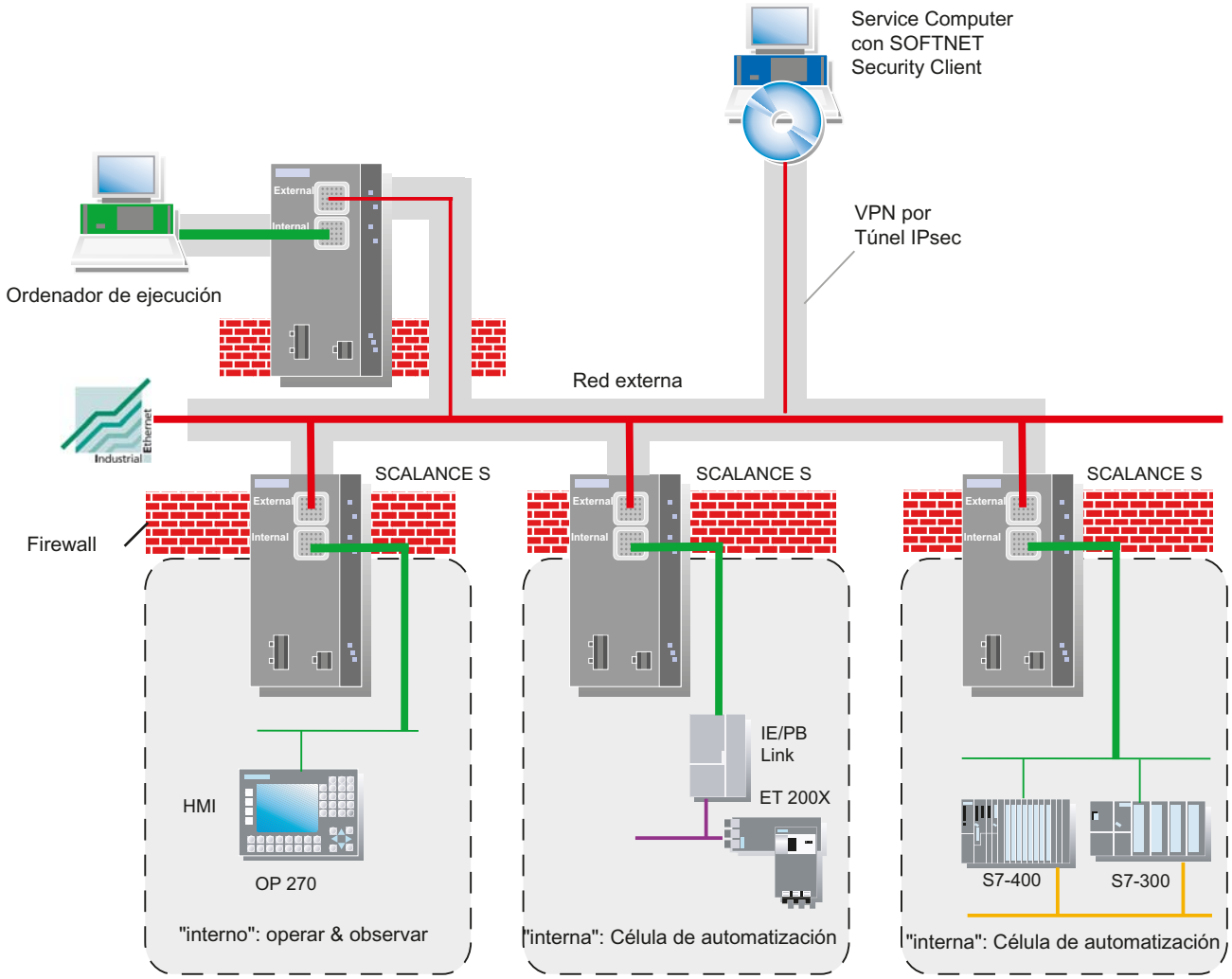
- Integridad

  Los datos intercambiados están protegidos de falseamientos.

- Autenticidad

  Sólo puede establecer un túnel quien cuente con la correspondiente autorización.

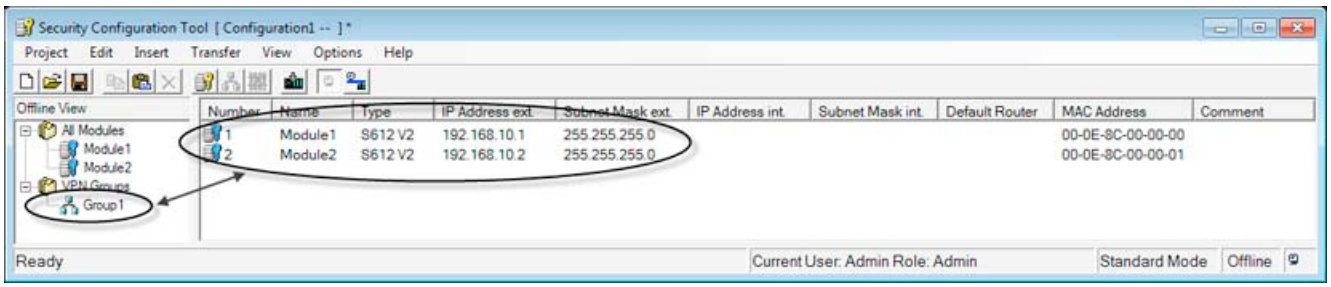
SCALANCE S utiliza el protocolo IPsec (modo túnel de IPsec) para la formación de túneles.



Las conexiones por túnel se realizan entre módulos del mismo grupo (VPN)

En el caso de SCALANCE S, las propiedades de una VPN se reúnen dentro de un grupo de módulos para todos los túneles IPsec.

Se establecen automáticamente túneles IPsec entre todos los módulos SCALANCE S y los módulos SOFTNET Security Client pertenecientes al mismo grupo.


Security Configuration Tool [Configuration1 --]*
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
VPN Groups
Group1
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 00-0E-8C-00-00-00
2 Module2 S612 V2 192.168.10.2 255.255.255.0 00-0E-8C-00-00-01
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

Módulos SCALANCE S pueden pertenecer paralelamente a diversos grupos en un proyecto.

ATENCIÓN
Si se cambia el nombre de un módulo SCALANCE S, se tienen que reconfigurar todos los módulos SCALANCE S de los grupos a los que pertenezca el módulo SCALANCE S modificado (comando **Transfer ▸ To All Modules...**). Si se cambia el nombre de un grupo, se tienen que reconfigurar todos los módulos SCALANCE S de ese grupo (comando **Transfer ▸ To All Modules...**).

ATENCIÓN
Telegramas Layer 2 sólo se transmiten vía túnel si entre dos módulos SCALANCE S no se encuentra ningún router. Regla general: Telegramas no IP sólo se transmiten a través de un túnel si los equipos que transmiten o reciben los telegramas se podían comunicar ya anteriormente, es decir, sin el uso de SCALANCE S. El que los modos de red se hayan podido comunicar o no antes del uso del SCALANCE S se determina a través de las redes IP en que se encuentran los equipos SCALANCE S. Si los SCALANCE S están en la misma subred IP, se parte de que los equipos terminales conectados en las redes protegidas de SCALANCE S se podían comunicar con telegramas no IP también antes del uso de SCALANCE S. Los telegramas no IP se transmiten entonces por túnel.

Método de autenticación

El método de autenticación se fija dentro de un grupo (de una VPN) y determina la forma de autenticación utilizada.

Son posibles métodos de autenticación basados en clave o en certificado:

- Preshared Keys

  La Preshared Key se distribuye a todos los módulos que se encuentren en el grupo.

  Para ello se introduce previamente en el campo "Preshared Key" del cuadro de diálogo "Group Properties" una contraseña a partir de la cual se genera esta clave.

- Certificado

  La autenticación basada en certificado denominada "Certificate" es el ajuste predeterminado, que está activado también en el Standard Mode. El comportamiento es el siguiente:

  – Al crear un grupo se genera automáticamente un certificado de grupo (= certificado CA).

  – Cada SCALANCE S existente en el grupo recibe un certificado signado con la clave del CA de grupo.

  Todos los certificados se basan en el estándar ITU X.509v3 (ITU, International Telecommunications Union).

  Los certificados son generados por una entidad certificadora contenida en la Security Configuration Tool.

ATENCIÓN
Restricción para el modo VLAN Dentro de un túnel VPN establecido con SCALANCE S no se transmite VLAN-Tagging. Razón: Los identificadores de VLAN contenidos en los telegramas (VLAN-Tags) se pierden, en el caso de los telegramas Unicast, al pasar por los SCALANCE S, ya que para la transmisión de los telegramas IP se utiliza IPSec. Por un túnel IPSec se transmiten sólo telegramas IP (no paquetes Ethernet), por lo que se pierde el tagging de VLAN. Como estándar no se pueden transmitir con IPSec telegramas Broadcast ni Mulitcast. En el caso de SCALANCE S, los IP-Broadcast se "empaquetan" y transmiten exactamente como paquetes MAC en UDP, inclusive con Ethernet-Header. Por ello se conserva también el VLAN-Tagging.

6.2 Grupos

6.2.1 Crear grupos y asignar módulos

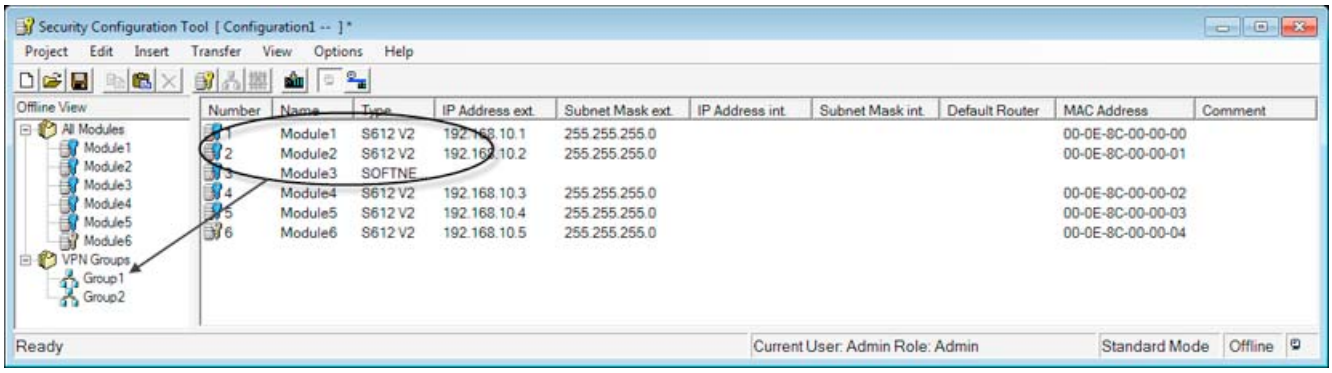
Procedimiento a seguir para configurar una VPN

Cree con el comando de menú:

Insert ▸ Group

un grupo.

Asigne al grupo los módulos SCALANCE S y SOFTNET Security Client que deban pertenecer a una red interna. Para ello, arrastre con el ratón el módulo al grupo deseado (arrastrar y colocar).


Security Configuration Tool [Configuration1 --] *
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
Module6
VPN Groups
Group1
Group2
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 00-0E-8C-00-00-00
2 Module2 S612 V2 192.168.10.2 255.255.255.0 00-0E-8C-00-00-01
3 Module3 SOFTNE
4 Module4 S612 V2 192.168.10.3 255.255.255.0 00-0E-8C-00-00-02
5 Module5 S612 V2 192.168.10.4 255.255.255.0 00-0E-8C-00-00-03
6 Module6 S612 V2 192.168.10.5 255.255.255.0 00-0E-8C-00-00-04
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

Configuración de propiedades

Como en el caso de la configuración de módulos, también en la configuración de grupos repercuten las dos vistas de operación seleccionables en la Security Configuration Tool:

(comando: **View ▸ Advanced Mode...**)

- **Standard Mode**

  En el Standard Mode se conservan los ajustes predeterminados por el sistema. También como persona no experta en IT puede configurar así túneles IPsec y practicar una comunicación de datos segura en su red interna.

- **Advanced Mode**

  El Advanced Mode le ofrece posibilidades para configurar de forma específica la comunicación por túnel.

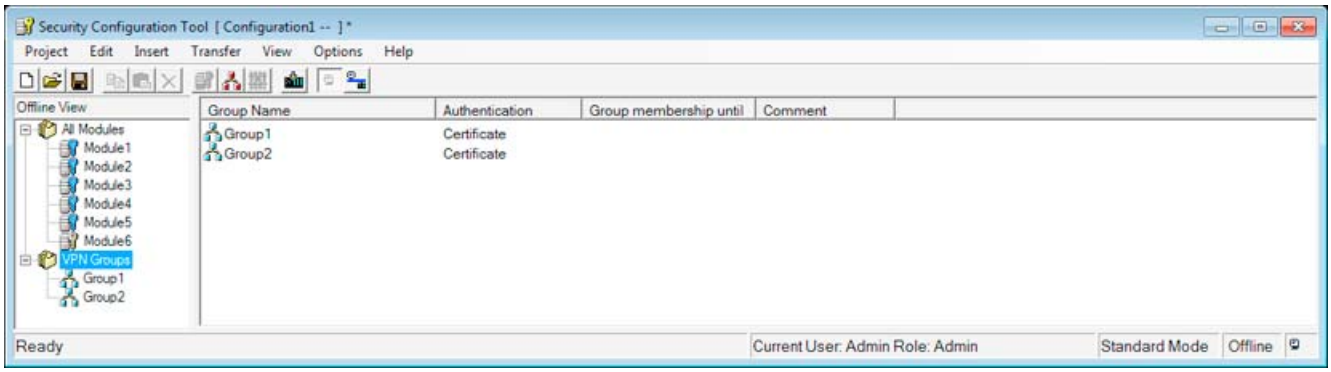
Nota

Parametrización de MD 740 / MD 741 o de otros VPN-Clients

Para la parametrización de MD 740 / MD 741 o de otros VPN-Clients se tienen que configurar propiedades VPN específicas del módulo en el modo extendido.

Visualización de todos los grupos configurados, con sus propiedades

Seleccione en el área de navegación "All Groups"



Se visualizan por columnas las siguientes propiedades de los grupos:

Tabla 6- 1 Propiedades de grupos

Propiedad/columna	Significado	Comentario/selección
Group Name	Nombre del grupo	de libre elección
Authentication	Tipo de autenticación	• Preshared Key • Certificate
Group membership until...	Duración de certificados	ver bajo
Comment	Comentario	de libre elección

Ajustar la duración de certificados

Abra de la forma siguiente el cuadro de diálogo en el que puede introducir la fecha de caducidad del certificado:

- haciendo un doble clic en un módulo de la ventana de propiedades o bien con el botón derecho del ratón, a través del comando **Properties**.

ATENCIÓN
Una vez caducado un certificado, se finaliza la comunicación a través del túnel.

6.2.2 Tipos de módulos dentro de un grupo

Tipos de módulos

Los siguientes tipos de módulos se pueden configurar en grupos con la Security Configuration Tool:

- SCALANCE S612
- SCALANCE S613

- SOFTNET Security Client
- MD 74x (sive para MD740-1 o MD741-1)

Reglas para la formación de grupos

Observe las reglas siguientes si desea formar grupos VPN:

- El primer módulo asignado a un grupo VPN decide qué otros módulos se pueden agregar.

  Si el primer equipo agregado está en el modo Routing, sólo se pueden agregar adicionalmente módulos con el Routing activado. Si el primer equipo agregado no está en el modo Bridge, sólo se pueden agregar adicionalmente módulos en el modo Bridge. Si se debe modificar el "modo" de un grupo VPN, se tienen que quitar todos los módulos contenidos en el grupo, agregándolos después de nuevo.

- No es posible agregar un módulo MD 740-1/MD 741-1 a un grupo VPN que contenga un módulo con el modo Brdige.

Vea en la tabla siguiente qué módulos se pueden reunir en un grupo VPN:

Módulo	Modo de operación del módulo ...	
	... en el modo Bridge	... en el modo Routing
S612 V1	x	-
S612 V2 *)	x	x
S613 V1	x	-
S613 V2 *)	x	x
SOFTNET Security Client 2005	x	-
SOFTNET Security Client 2008	x	x
SOFTNET Security Client V3.0	x	x
MD 74x	-	x

6.3 Configuración de túnel en el Standard Mode

Propiedades de grupo

En el Standard Mode son válidas las siguientes propiedades:

- Todos los parámetros de los túneles IPsec y el método de autenticación están predeterminados.

  En el cuadro de diálogo para el grupo se pueden visualizar los valores estándar ajustados.

- El modo de aprendizaje está activado para todos los módulos.

Abrir el cuadro de diálogo para visualización de valores estándar

Estando seleccionado el grupo, seleccione el siguiente comando de menú:

Edit ▸ Properties...

La visualización es idéntica al del cuadro de diálogo en el Advanced Mode; pero los valores no se pueden modificar.

6.4 Configuración de túnel en el Advanced Mode

El Advanced Mode le ofrece posibilidades para configurar de forma específica la comunicación por túnel.

Conmmutar al Advanced Mode

Para todas las funciones descritas en este capítulo, conmute el modo de funcionamiento con el siguiente comando de menú:

View ▸ Advanced Mode

Nota

Una conmutación realizada al Advanced Mode para el proyecto actual ya no se puede anular.

A no ser que salga del proyecto sin guardar y lo abra de nuevo.

6.4.1 Configuración de propiedades de grupo

Propiedades de grupo

En la vista de operación "Advanced Mode" se pueden configurar las siguientes propiedades de grupo:

- Método de autenticación
- Ajustes IKE (área de diálogo: Advanced Settings Phase 1)
- Ajustes IPsec (área de diálogo: Advanced Settings Phase 2)

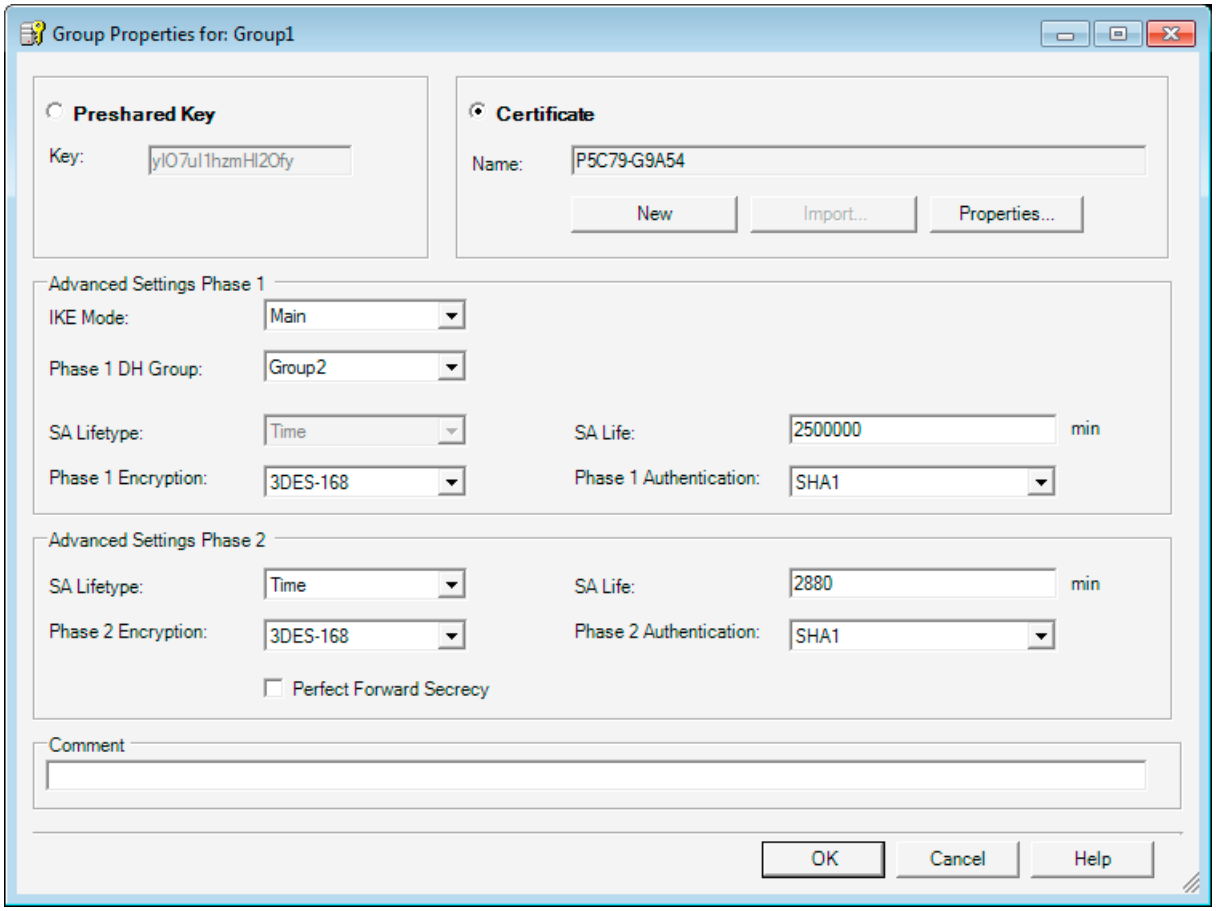
ATENCIÓN
Para poder ajustar estos parámetros necesita tener conocimientos en materia de IPsec.

Si no efectúa o modifica ningún ajuste, rigen los ajustes predeterminados del Standard Mode.

Abrir el cuadro de diálogo para entrada de propiedades de grupo

- Estando seleccionado el grupo, seleccione el siguiente comando de menú:

  Edit ▸ Properties...



Parámetros para ajustes ampliados Fase 1 - Ajustes IKE

Fase 1: Cambio de clave (IKE, Internet Key Exchange):

Aquí puede ajustar parámetros para el protocolo de gestión de claves IPsec. El cambio de clave tiene lugar por medio del procedimiento estandarizado IKE.

Se pueden ajustar los siguientes parámetros de protocolo IKE:

Tabla 6- 2 Parámetros de protocolo IKE (grupo de parámetros "Advanced Settings Phase 1'" en el diálogo)

Parámetros	Valores/selección	Comentario
IKE Mode	• Main Mode • Aggressive Mode	Método de cambio de clave La diferencia entre la modalidad Main y Aggressive es la "Identity-Protection" que se utiliza en el Main Mode. La identidad se transmite codificada en el Main Mode, en el Aggressive Mode no.
Phase 1 DH Group Phase 1 DH Group	• Group 1 • Group 2 • Group 5	Convenio de codificación Diffie-Hellman: Grupos Diffie-Hellman (algoritmos criptográficos seleccionables en el protocolo de cambio de claves Oakley)
SA Lifetype SA Lifetype	• Time	Phase 1 Security Association (SA) • Limitación de tiempo (min., default: 2500000) Se limita el tiempo de vida útil para el material de codificación actual. Una vez transcurrido ese tiempo se negocia de nuevo el material de codificación.
SA Life SA Life	Valor numérico	("Time"→min.,) Rango de valores: 1440...2 500 000
Phase 1 Encryption Phase 1 Encryption	• DES • 3DES-168 • AES-128 • AES-192 • AES-256	Algoritmo de codificación • Data Encryption Standard (longitud de código 56 bit, modo CBC) • DES triple (longitud de código 168 bit, modo CBC) • Advanced Encryption Standard (longitud de código 128 bit, 192 Bit o 256 Bit, modo CBC)
Phase 1 Authentication Phase 1 Authentication	• MD5 • SHA1	Algoritmo de autenticación • Message Digest Version 5 • Secure Hash Algorithm 1

Parámetros para Advanced Settings Phase 2 - Ajustes IPSec

Fase 2: Intercambio de datos (ESP, Encapsulating Security Payload)

Aquí puede ajustar parámetros para el protocolo de intercambio de datos IPsec. El intercambio de datos tiene lugar por medio del protocolo de seguridad estandarizado ESP.

Se pueden ajustar los siguientes parámetros de protocolo ESP:

Tabla 6- 3 Parámetros de protocolo IPsec (grupo de parámetros "Advanced Settings Phase 2'" en el diálogo)

Parámetros	Valores/selección	Comentario
SA Lifetype SA Lifetype	• Time	Phase 2 Security Association (SA) • Limitación de tiempo (min., default: 2880) Se limita el tiempo de vida útil para el material de codificación actual. Una vez transcurrido ese tiempo se negocia de nuevo el material de codificación.
	• Limit	• Volumen de datos limitado (mByte, Default 4000)
SA Life SA Life	Valor numérico	("Time"→min., "Limit" → mByte) Rango de valores (Time): 1440...16 666 666 Rango de valores (Limit): 2000...500 000
Phase 2 Encryption Phase 2 Encryption	• 3DES-168 • DES • AES-128	Algoritmo de codificación • DES triple especial (longitud de código 168 bit, modo CBC) • Data Encryption Standard (longitud de código 56 bit, modo CBC) • Advanced Encryption Standard (longitud de código 128 bit, modo CBC)
Phase 2 Authentication Phase 2 Authentication	• MD5 • SHA1	Algoritmo de autenticación • Message Digest Version 5 • Secure Hash Algorithm 1
Perfect Forward Secrecy	• On • Off	Antes de cada negociación de una IPsec-SA tiene lugr una nueva negociación de la clave con ayuda del procedimiento Diffie-Hellman.

6.4.2 Inclusión del SCALANCE S en un grupo configurado

Las propiedades de grupo configuradas se adoptan para SCALANCE S nuevos que se incluyen en un grupo existente.

Procedimiento a seguir

Dependiendo de que las propiedades de grupo se hayan modificado o no, se tiene que prodecer de forma distinta:

- **Caso a:** No se han modificado las propiedades del grupo

1. Agregue los nuevos SCALANCE S al grupo.
2. Cargue la configuración en los nuevos módulos.

- **Caso b:** Se han modificado las propiedades del grupo

1. Agregue los nuevos SCALANCE S al grupo.
2. Cargue la configuración en todos los módulos pertenecientes al grupo.

Ventaja

No es necesario configurar de nuevo ni cargar SCALANCE S ya existentes, puestos en servicio. No resulta ninguna influenciación ni interrupción de la comunicación en curso.

6.4.3 SOFTNET Security Client

Ajustes compatibles para SOFTNET Security Client

Tenga en cuenta las siguientes peculiaridades si incorpora al grupo configurado módulos del tipo SOFTNET Security Client:

Parámetros	Ajuste / peculiaridad
Phase 1 DH Group Phase 1 DH Group	DH Group 1 y 5 sólo se puede utilizar para la comunicación entre los módulos SCALANCE S.
Phase 1 Encryption Phase 1 Encryption	No son posibles DES, AES-128 ni AES-192.
Phase 1 Authentication Phase 1 Authentication	No es posible MD5.
Fase 1 - duración SA Fase 1 - duración SA	Rango de valores: 1440...2879 (sólo SOFTNET Security Client V3.0)
SA Lifetype SA Lifetype	Se tiene que seleccionar idéntico para ambas fases.
Phase 2 Encryption Phase 2 Encryption	No es posible AES-128.
Fase 2 - duración SA Fase 2 - duración SA	Rango de valores: 1440...2879 (sólo SOFTNET Security Client V3.0)
Phase 2 Authentication Phase 2 Authentication	No es posible MD5.

ATENCIÓN

Los ajustes de los parámetros para una configuración de SOFTNET Security Client deben corresponder con las propuestas por defecto o Default Proposals de los módulos SCALANCE S ya que un SOFTNET Security Client se encuentra la mayoría de las veces en una aplicación o uso móvil, con lo que su recibe su dirección IP de forma dinámica, con lo que el SCALANCE S sólo puede admitir una conexión a través de estas Default Proposals o propuestas por defecto.

Deberá ocuparse igualmente de que sus ajustes de Phase 1 correspondan con una de las dos propuestas siguientes para poder construir un túnel con un SCALANCE S.

Si utiliza otros ajustes en la Security Configuration Tool, entonces, la comprobación de coherencia detecta un fallo de coherencia al intentar una derivación de la configuración. Así, no podrá usted derivarse de su configuración del SOFTNET Security Client hasta que haya adaptado los ajustes según corresponda.

Authentication	IKE Mode	Grupo DH	Codificación	Hash	Duración (Min)
Certificado	Main mode (modo principal)	Grupo DH 2	3DES-168	SHA1	1440…2879
Preshared Keys	Main mode (modo principal)	Grupo DH 2	3DES-168	SHA1	1440…2879
Certificado	Main mode (modo principal)	Grupo DH 2	AES256	SHA1	1440…2879

6.4.4 Configurar propiedades VPN específicas del módulo

Para el intercambio de datos a través de túnel IPsec en VPN se pueden configurar las siguientes propiedades específicas del módulo:

- Dead-Peer-Detection
- Permiso para iniciar el establecimiento de la conexión
- Dirección IP pública para comunicación a través de Internet Gateways

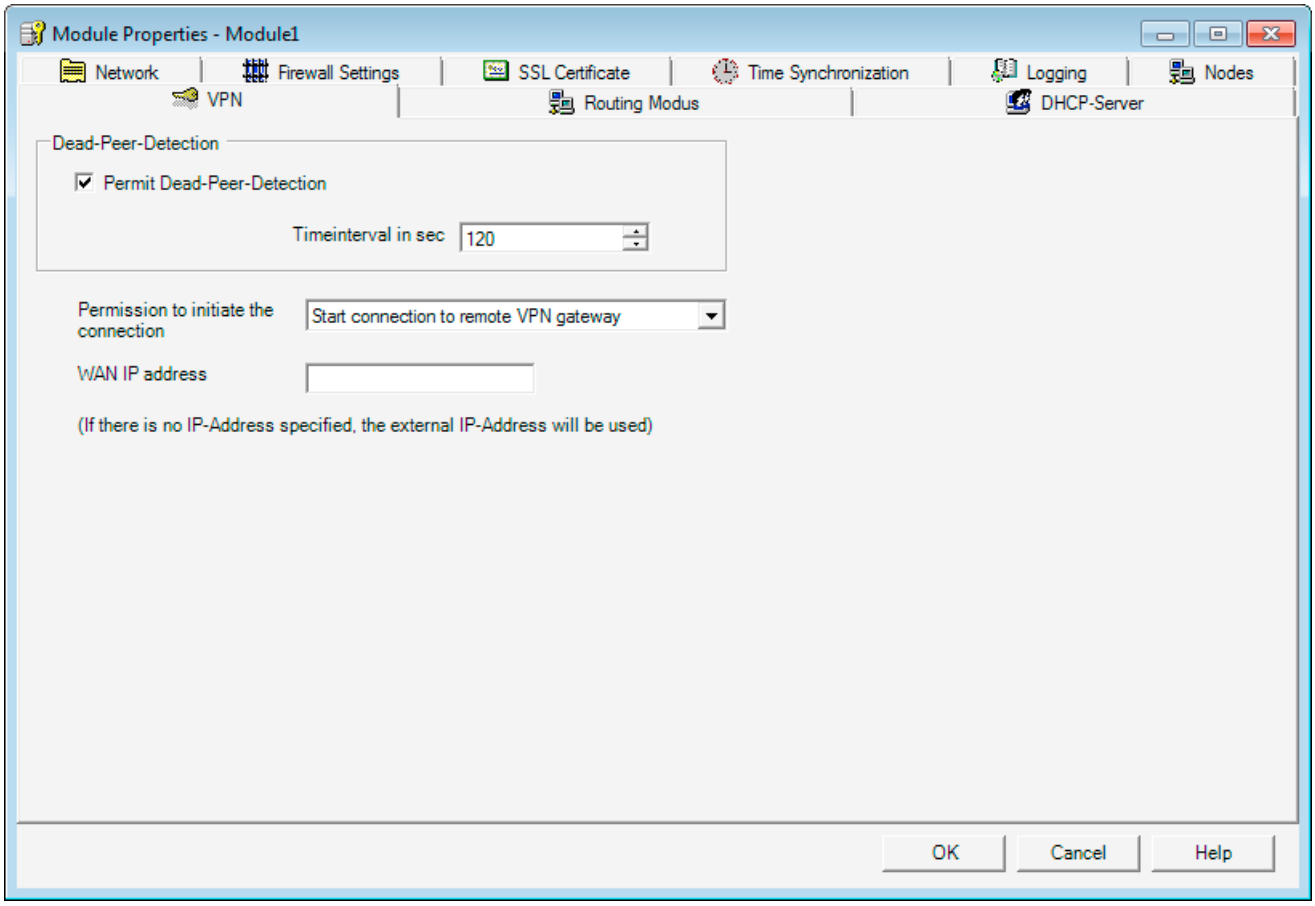
Abrir el cuadro de diálogo para configuración de propiedades de módulo VPN

Marque el módulo a editar y seleccione el siguiente comando de menú en el modo Extended:

Edit ▸ Properties..., ficha "VPN"

Nota

La ficha "VPN" sólo se puede seleccionar si el módulo a configurar se encuentra en un grupo VPN.



Dead-Peer-Detection (DPD)

Estando activado DPD, los módulos intercambian mensajes adicionales a intervalos de tiempo ajustables. Con esto se puede reconocer si aún existe una conexión en VPN. Si ya no existe, se finalizan prematuramente las "Security Associations" (SA). Estando desactivado DPD, la "Security Association" (SA) sólo finaliza tras expirar su duración de SA (ajuste de la duración de SA: ver la configuración de las propiedades del grupo).

Como estándar está activado DPD.

Permiso para iniciar el establecimiento de la conexión

Puede limitar el permiso para iniciar el establecimiento de la conexión de VPN a determinados módulos en VPN.

El factor decisivo para el ajuste del parámetro aquí descrito es la asignación de la dirección IP para el gateway del módulo a proyectar aquí. En el caso de una dirección IP asignada estáticamente, el módulo puede ser encontrado por el interlocutor. En el caso de una dirección IP asignada dinámicamente, y por lo tanto constantemente cambiante, el interlocutor no puede establecer sin más una conexión.

Modo	Significado
Iniciando conexión con interlocutor (predeterminado)	Con esta opción, el módulo está "activo", es decir, intenta establecer una conexión con el interlocutor. Esta opción se recomienda si el proveedor asigna una dirección IP dinámica para el gateway del módulo SCALANCE S que se debe configurar aquí. El direccionamiento del interlocutor tiene lugar a través de su dirección WAN IP configurada o de su dirección IP de módulo externo.
Esperando a interlocutor	Con esta opción, el módulo está "pasivo", es decir, espera a que el interlocutor establezca una conexión. Esta opción se recomienda si el proveedor asigna una dirección IP estática para el gateway del módulo que se debe configurar aquí. Con esto se consigue que sólo el interlocutor intente establecer la conexión.

ATENCIÓN
No ponga todos los módulos de un grupo VPN a "Esperando al interlocutor", pues de hacerlo no se establece ninguna conexión.

Dirección IP WAN - direcciones IP de los módulos y gateways en una VPN vía Internet

En caso de operar una VPN con túnel IPsec a través de Internet se necesitan, por regla general, direcciones IP adicionales para los Internet Gateways como por ejemplo DSL-Router. Los distintos módulos SCALANCE S o MD 740-1 / MD 741-1 tienen que conocer las direcciones IP externas de los módulos interlocutores en la VPN.

Nota

Si utiliza un DSL-Router como Internet Gateway, tiene que activar en él al menos los puertos siguientes:

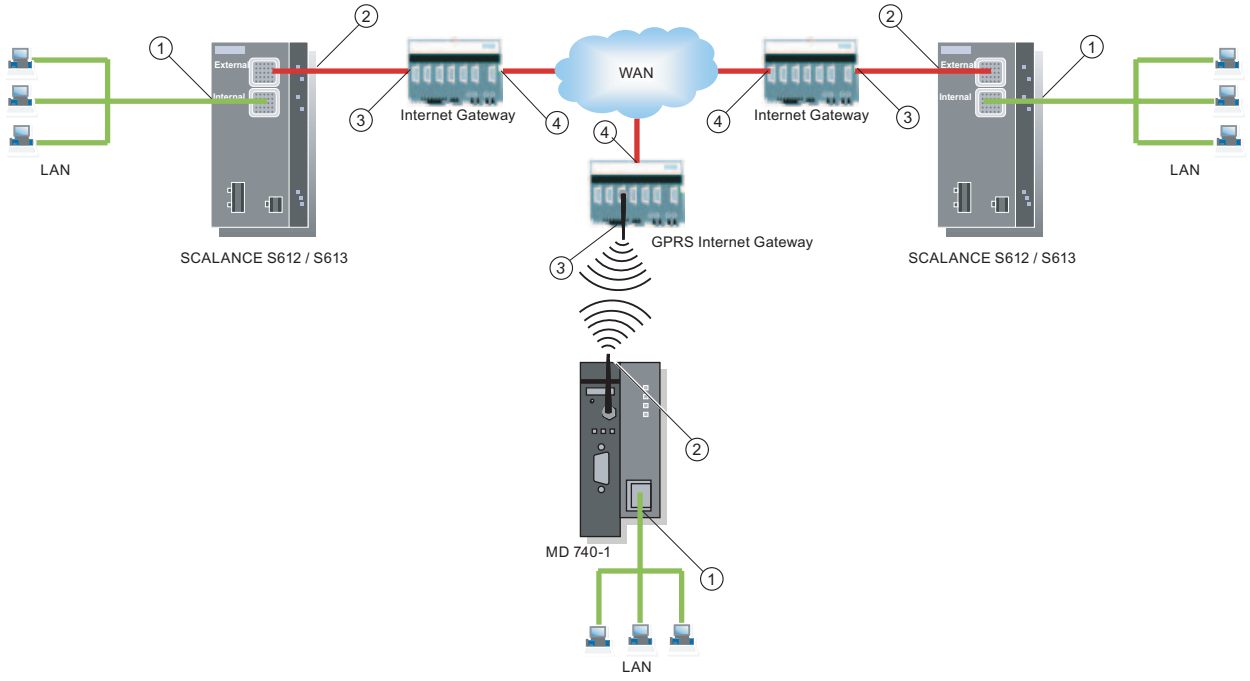
- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

Si se descargan configuraciones (a través del WAN sin túnel activo) se tiene que activar además el Port 443 (HTTPS).

Para esto se tiene la posibilidad de asignar en la configuración del módulo esta dirección IP externa como "dirección IP WAN". Al cargar la configuración del módulo se comunican entonces a los módulos estas direcciones IP WAN de los módulos interlocutores.

Si no se asigna ninguna dirección IP WAN, se utiliza la dirección IP externa del módulo.

La representación siguiente aclara la relación de las direcciones IP.



① Dirección IP interna - de un módulo
② Dirección IP externa - de un módulo
③ Dirección IP interna - de un Internet Gateway (p. ej. GPRS-Gateway)
④ Dirección IP externa (dirección IP WAN) - de un Internet Gateway (p. ej. DSL-Router)

6.5 Configuración de nodos de red internos

Para que los socios de túneles puedan dar a conocer sus propios nodos internos, un SCALANCE S debe conocer sus propios nodos internos. Además debe también conocer los nodos internos del SCALANCE S junto a los cuales se encuentra dentro de un grupo. Esta información se utiliza en un SCALANCE S para determinar qué paquete de datos se debe transmitir por qué túnel.

En redes planas, SCALANCE S ofrece la posibilidad de programar los nodos de red automáticamente por aprendizaje o de configurarlos estáticamente.

En el modo Routing se dotan de túnel subredes completas; allí no es necesario aprender ni configurar de forma estática los nodos de red.

6.5.1 Funcionamiento del modo de aprendizaje

Localización automática de nodos para la comunicación vía túnel (sólo modo Bridge)

Una gran ventaja para la configuración y el trabajo de la comunicación vía túnel es que SCALANCE S puede localizar por sí mismo nodos en la red interna.

Nuevos nodos son reconocidos por SCALANCE S durante el funcionamiento en curso. Los nodos detectados se notifican a los módulos SCALANCE S pertenecientes al mismo grupo. Con esto está garantizado en todo momento el intercambio de datos en ambos sentidos dentro de los túneles de un grupo.

Requisitos

Se reconocen los siguientes nodos:

- Nodos de red aptos para IP

  Se encuentran nodos de red aptos para IP si envían una respuesta ICMP al ICMP-Subnet-Broadcast.

  Nodos IP situados detrás de routers se pueden encontrar si los routers transmiten ICMP-Broadcasts.

- Nodos de red ISO

  Nodos de red que no sean aptos para IP, pero que se puedan interrogar a través de protocolo ISO, también se pueden programar por aprendizaje.

  Condición para ello es que respondan a telegramas XID o TEST. TEST y XID (Exchange Identification) son protocolos auxiliares para el intercambio de informaciones en el nivel Layer 2. A través del envío de estos telegramas con una dirección Broadcast se pueden localizar estos nodos de red.

- Nodos PROFINET

  Con ayuda de DCP (Discovery and basic Configuration Protocol) se encuentran nodos PROFINET.

Nodos de red que no cumplan estos requisitos se tienen que configurar.

Subredes

También se tienen que configurar subredes que se encuentren detrás de routers internos.

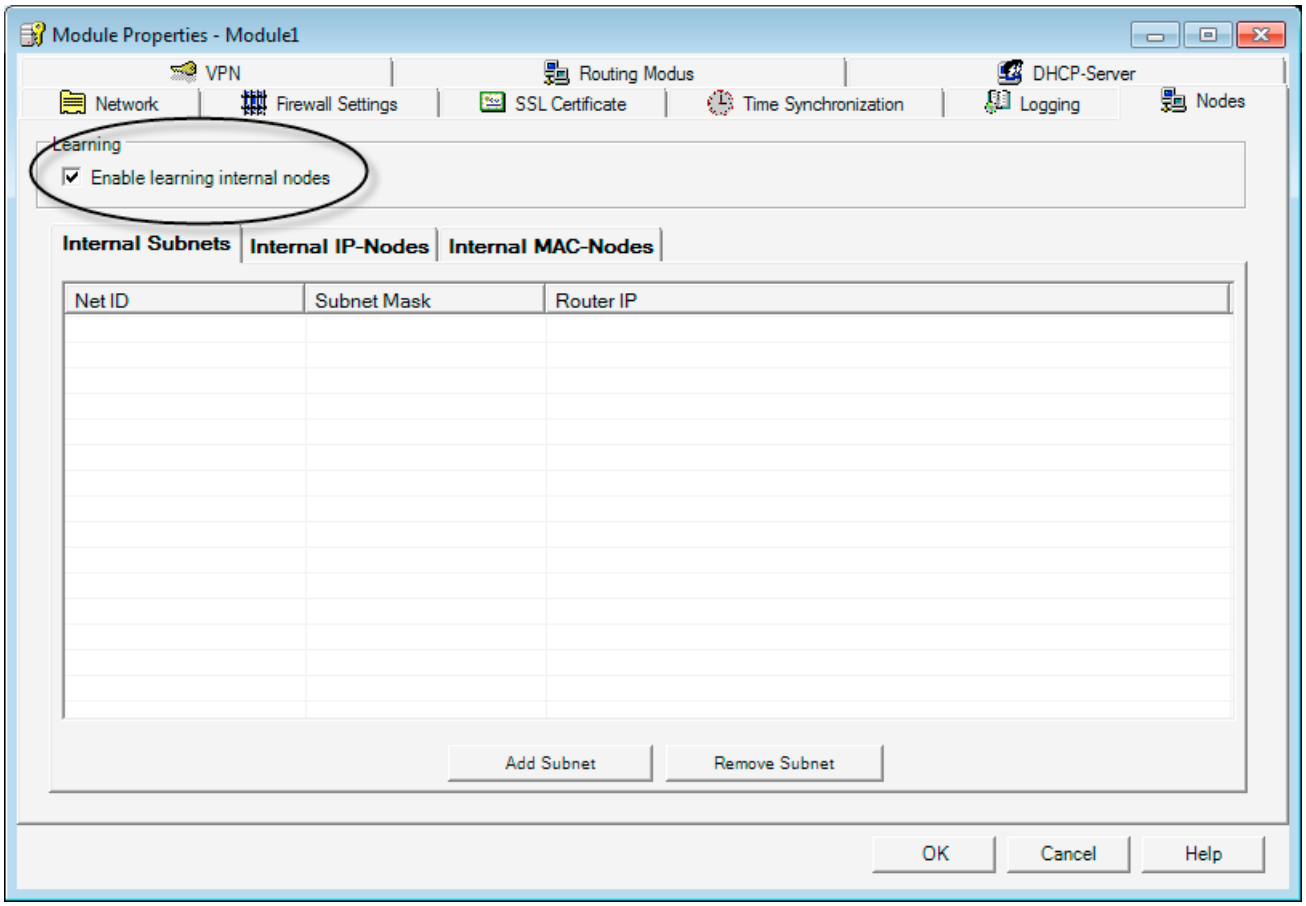
Activación y desactivación del modo de aprendizaje

La función de aprendizaje está activada como estándar para cada módulo SCALANCE S en caso de configuración con la herramienta Security Configuration Tool.

La programación por aprendizaje también se puede desactivar por completo. Entonces se tienen que configurar manualmente todos los nodos internos que participen en la comunicación vía túnel.

El cuadro de diálogo en el que se puede seleccionar la opción se abre de la siguiente forma:

- Con el modo seleccionado a través del comando
  Edit ▸ Properties..., ficha "Node"



¿Cuándo es conveniente desactivar el modo de aprendizaje automático?

Los ajustes estándar para SCALANCE S parten de que las redes internas son siempre "seguras"; esto significa también que normalmente no se conectan a la red interna nodos de red que no sean dignos de confianza.

La desactivación del modo de aprendizaje puede ser conveniente si la red interna es estática, es decir, si no cambian el número ni las direcciones de los nodos internos.

Con la desconexión del modo de aprendizaje se suprime en la red interna la carga que los telegramas de programación por aprendizaje suponen para el medio y los nodos. También aumentan en cierta medida las prestaciones del SCALANCE S, ya que no está recargado por el procesamiento de los telegramas de programación por aprendizaje.

Observación: En el modo de aprendizaje se registran todos los nodos de la red interna. Los datos relativos a los recursos de la VPN se refieren sólo a los nodos que se comuniquen en la red interna a través de VPN.

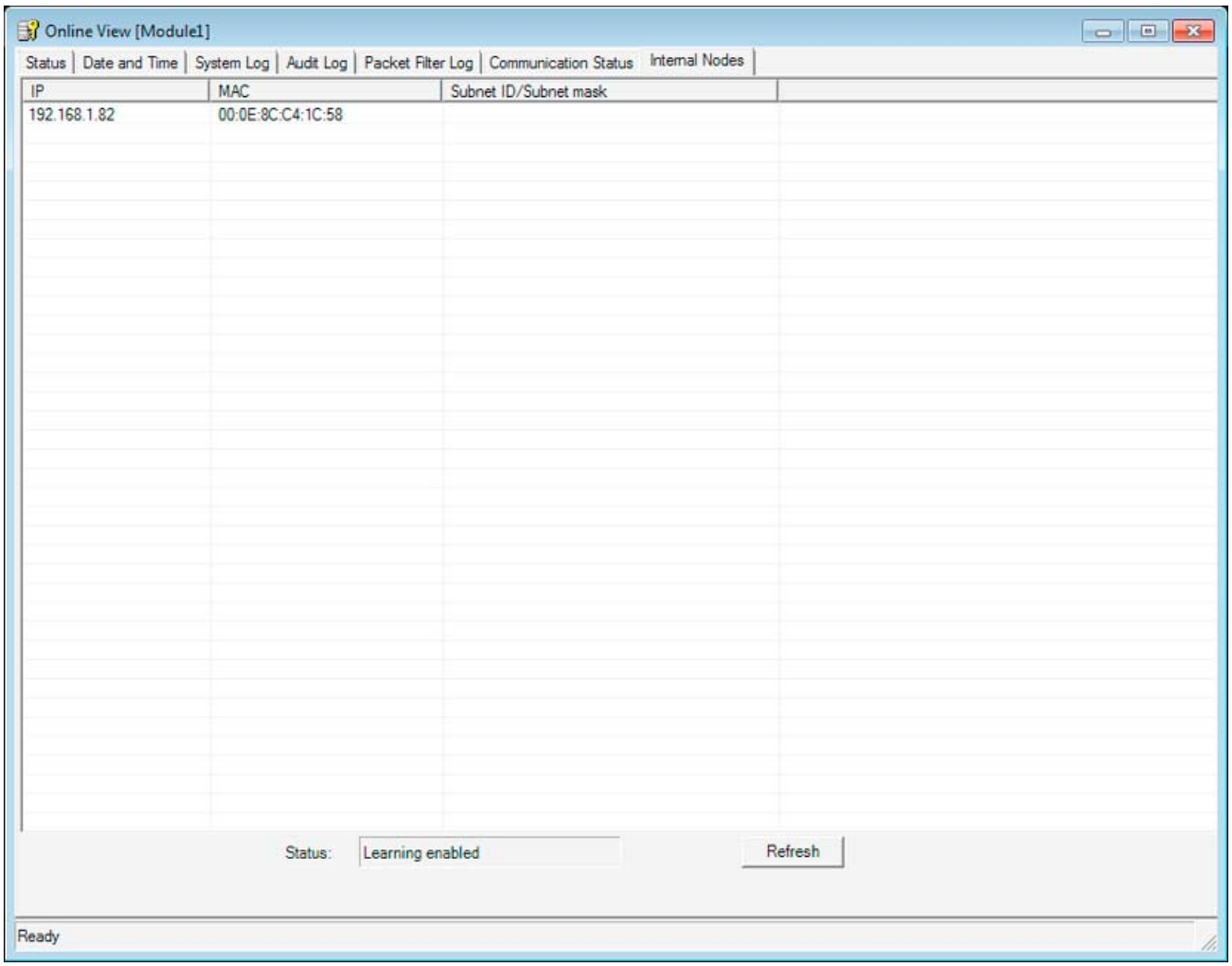
ATENCIÓN
Si en la red interna se utilizan más de 64 (para SCALANCE S613) o 32 (para SCALANCE S612) nodos internos, se sobrepasa con esto la cantidad de recursos admisible y se crea un estado operativo no permitido. Debido a la dinámica en el tráfico de red ocurre entonces que nodos internos ya programados por aprendizaje son reemplazados por nuevos nodos internos, hasta ahora desconocidos.

6.5.2 Visualización de los nodos de red internos encontrados

Todos los nodos de red encontrados se pueden visualizar en la Security Configuration Tool, en el modo "Online", en la ficha "Internal Nodes".

Llame el siguiente comando de menú:

Edit ▸ Online Diagnostics…



6.5.3 Configuración manual de nodos de red

Nodos de red no programables

Existen en la red interna nodos que no se pueden programar por aprendizaje. Estos nodos se tienen que configurar. Aquí tiene que activar el Advanced Mode en la Security Configuration Tool.

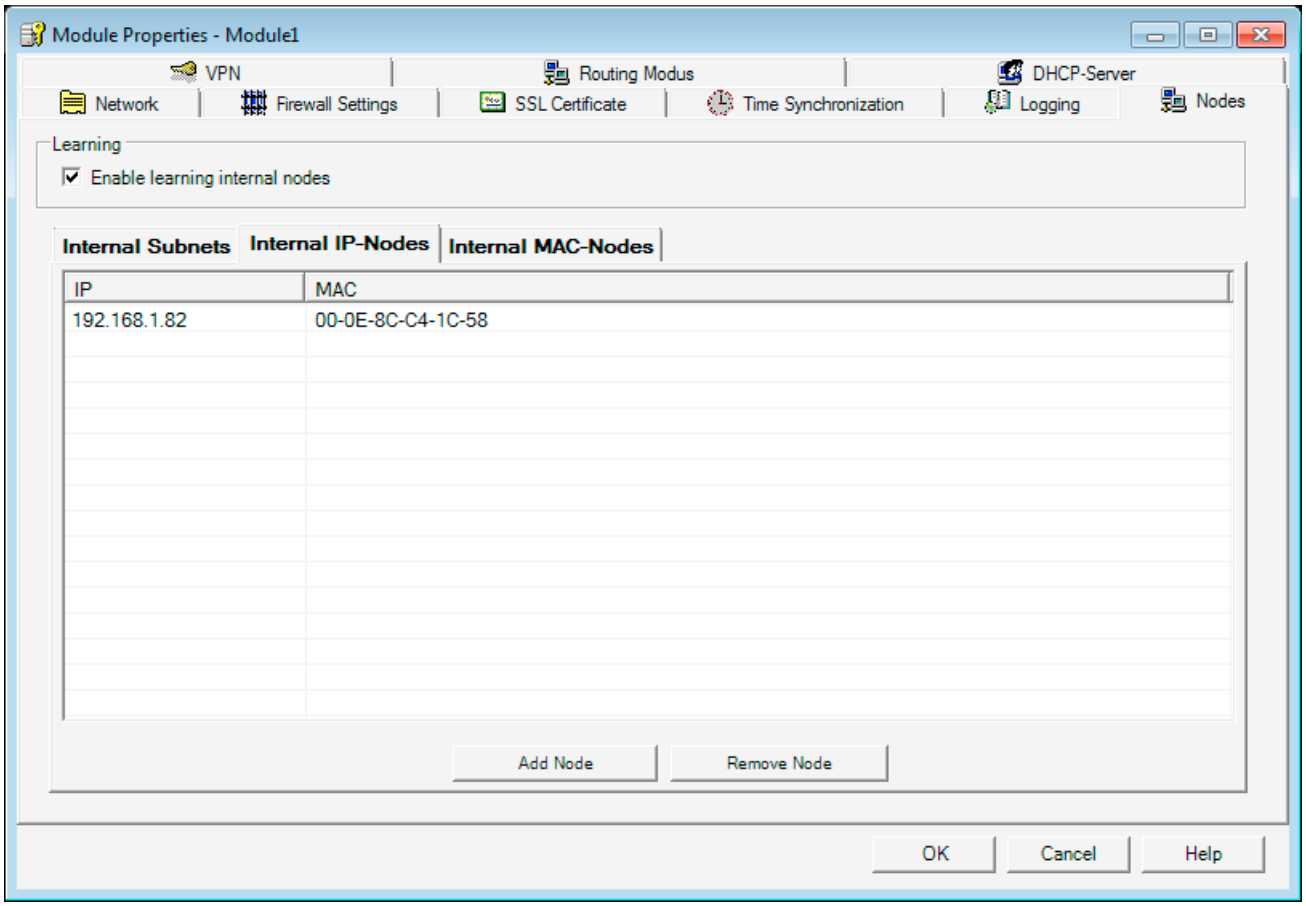
También se tienen que configurar subredes que se encuentren en la red interna del SCALANCE S.

Cuadro de diálogo / ficha

El cuadro de diálogo en el que se pueden configurar los nodos de red se abre de la siguiente forma:

- Con el modo seleccionado a través del comando

  Edit ▸ Properties..., ficha "Node"



Introduzca en las fichas aquí seleccionables los parámetros de dirección requeridos en cada caso para todos los nodos de red que deban ser protegidos por el módulo SCALANCE S seleccionado.

Ficha "Internal IP-Nodes" (sólo en el modo bridge)

Parámetros configurables: Dirección IP y, como opción, la dirección MAC

Ficha "Internal MAC-Nodes" (sólo en el modo bridge)

Parámetros configurables: Dirección MAC

Ficha "Internal Subnets"

En caso de una subred interna (un router en la red interna) se tienen que indicar los siguientes parámetros de dirección:

Parámetros	Función	Valor de ejemplo
Network ID	ID de la subred: en base al ID de la subred, el router reconoce si una dirección de destino está en la subred o fuera de la misma.	196.80.96.0
Subnet mask	Máscara de subred: la máscara de subred estructura la red y sirve para formar el ID de la subred.	255.255.255.0
Router IP	Dirección IP del router	196.80.96.1

Efecto al utilizar SOFTNET Security Client

Si al utilizar SCALANCE S612 / S613 tiene que configurar estaciones estáticamente, tal como se ha descrito, tiene que cargar también de nuevo la configuración para un SOFTNET Security Client empleado en el grupo VPN.

SOFTNET Security Client (S612/S613) 7

Con el software de PC SOFTNET Security Client son posibles accesos remotos del PC/PG a equipos de automatización protegidos por SCALANCE S, más allá de los límites de redes públicas.

Este capítulo describe cómo se realiza la configuración del SOFTNET Security Client en la Security Configuration Tool y cómo se pone a continuación en servicio en el PC/PG.

Otras informaciones

La ayuda online del SOFTNET Security Client le proporcionará también información detallada sobre los diálogos y los parámetros ajustables.

Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

Consulte también

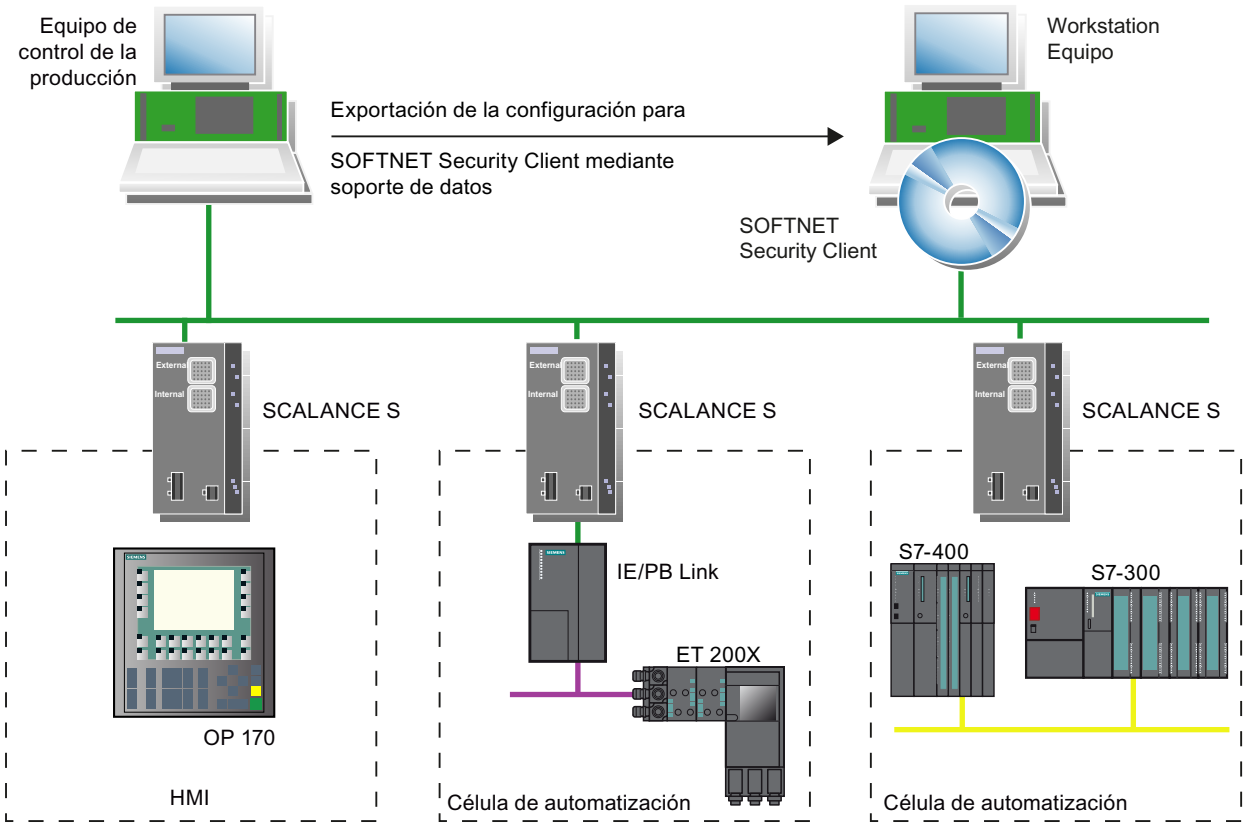
Comunicación segura en la VPN a través de túnel IPsec (S612/S613) (Página 179)

7.1 Uso de SOFTNET Security Client

Campo de aplicación - acceso a través de VPN

Mediante el SOFTNET Security Client se configura automáticamente un PC/PG de manera que pueda establecer con uno o varios SCALANCE S una comunicación túnel IPsec protegida en la VPN (Virtual Private Network).

Aplicaciones de PG/PC, como por ejemplo Diagnóstico NCM o STEP7, pueden acceder así a través de una conexión túnel protegida a equipos o redes que se encuentren en una red interna protegida por SCALANCE S.



Comunicación automática a través de VPN

Importante para su aplicación es que el SOFTNET Security Client reconozca por sí mismo cuándo se produce un acceso a la dirección IP de una estación participante en la VPN La estación se direcciona simplemente a través de la dirección IP, como si se encontrara en la subred local en la que está conectado también el PC/PG provisto de la aplicación.

ATENCIÓN
Tenga en cuenta que a través del túnel IPSec sólo puede tener lugar comunicación basada en IP entre SOFTNET Security Client y SCALANCE S.

Manejo

El software de PC SOFTNET Security Client posee una superficie de operación de fácil manejo para configuración de las propiedades de Security necesarias para la comunicación con equipos protegidos por SCALANCE S. Tras la configuración, el SOFTNET Security Client funciona en segundo plano, siendo esto visible por un icono en el SYSTRAY del PG/PC.

Detalles en la ayuda online

Encontrará también informaciones detalladas sobre los cuadros de diálogo y los campos de introducción en la ayuda online de la interfaz de operación del SOFTNET Security Client.

A la ayuda online se accede por medio del botón "Help" o con la tecla F1.

¿Cómo funciona el SOFTNET Security Client ?

El SOFTNET Security Client carga por lectura la configuración creada con la herramienta de configuración Security Configuration Tool y determina, sobre la base del archivo, los certificados a importar.

El Root-Certificate y las Private Keys se importan y se almacenan en el PG/PC local.

A continuación se realizan, con los datos de la configuración, ajustes de Security para que las aplicaciones puedan acceder a direcciones IP que se encuentren detrás de módulos SCALANCE-S.

Si está activado el modo de aprendizaje para las estaciones o los equipos de automatización internos, el módulo de configuración establece primero una directiva de seguridad para el acceso a módulos SCALANCE S. SOFTNET Security Client interroga a continuación los módulos SCALANCE S para determinar las direcciones IP de las respectivas estaciones internas.

SOFTNET Security Client registra esas direcciones IP en listas de filtros especiales de esa directiva de seguridad. Después de esto, aplicaciones como por ejemplo STEP 7 se pueden comunicar con los equipos de comunicación a través de VPN.

ATENCIÓN
En un sistema Windows, las directivas de seguridad IP están archivadas en forma personalizada. Para cada usuario sólo puede ser válida una única directiva de seguridad IP. Si una directiva de seguridad IP existente no dese ser sobrescrita por la instalación del SOFTNET Security Client, debería efectuar por ello la instalación y el uso del SOFTNET Security Client bajo un usuario creado ex profeso para ello.

Entorno de uso

El SOFTNET Security Client está previsto para el uso con el sistema operativo Windows XP SP2 y SP3 (no "Home-Edition") y Windows 7 (no "Home-Edition").

Comportamiento en caso de problemas

Si se presentan problemas en el PG/PC, SOFTNET Security Client reacciona del siguiente modo:

- las directivas de seguridad establecidas se conservan también después de desconectar y volver a conectar el PG/PC;
- en caso de una configuración incorrecta se emiten mensajes.

7.2 Instalación y puesta en servicio del SOFTNET Security Client

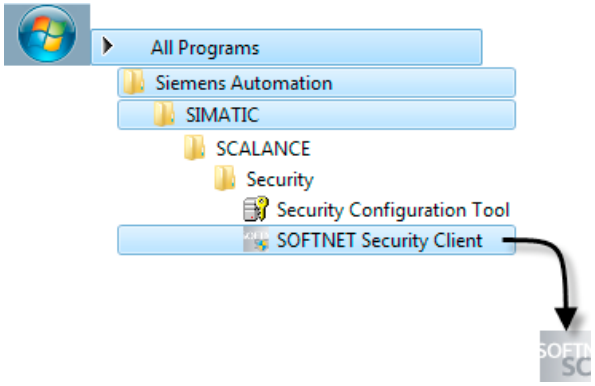
7.2.1 Instalación e inicio de SOFTNET Security Client

El software de PC SOFTNET Security Client se instala desde el CD SCALANCE S.

1. Lea primero lo dicho en el archivo README de su CD SCALANCE S y tenga en cuenta eventuales instrucciones adicionales para la instalación.
2. Ejecute el programa Setup.

   Lo más sencillo es que para ello abra el índice de su CD SCALANCE S → se inicia automáticamente al introducir el CD o bien se puede abrir a través del archivo start_exe. Seleccione entonces directamente la entrada "Installation SOFTNET Security Client"

Tras la instalación y el inicio de SOFTNET Security Client aparce el iconos de SOFTNET Security Client en la barra de tareas de Windows:



Configuración de SOFTNET Security Client

Una vez activadas, las funciones más importantes se desarrollan en segundo plano en el PG/PC.

La configuración de SOFTNET Security Client tiene lugar en dos pasos:

- Exportación de una configuración de Security desde la herramienta de configuración SCALANCE S Security Configuration Tool.
- Importación de la configuración de Security en la superficie propia, tal como se describe en el apartado siguiente.

Comportamiento de arranque

Para una configuración al grado máximo, el SOFTNET Security Client necesita, debido al sistema, hasta 15 para la carga de las reglas de seguridad. La CPU de su PG/PC se utiliza al 100% de su rendimiento durante ese tiempo.

Salir de SOFTNET Security Client - repercusiones

Si se sale de SOFTNET Security Client se desactiva también la directiva de seguridad.

Es posible salir de SOFTNET Security Client del siguiente modo:

- con el comando de menú en el SYSTRAY de Windows; seleccione con el botón derecho del ratón el icono de SOFTNET Security Client y seleccione la opción "Shut Down SOFTNET Security Client".
- estando abierta la superficie, con el botón "Quit".

7.2.2 Desinstalación de SOFTNET Security Client

Al realizar la desinstalación se reponen al estado original las propiedades de Security ajustadas por el SOFTNET Security Client.

7.3 Crear un archivo de configuración con la herramienta de configuración Security Configuration Tool

Configuración del módulo SOFTNET Security Client en el proyecto

El SOFTNET Security Client se habilita en el proyecto como módulo. A diferencia de los módulos SCALANCE S no se tienen que configurar otras propiedades.

Simplemente se asigna el módulo SOFTNET Security Client al grupo o a los grupos de módulos en los que se deben establecer túneles IPsec para comunicación con el PC/PG.

Entonces son determinantes las propiedades de grupo que usted haya configurado para esos grupos.

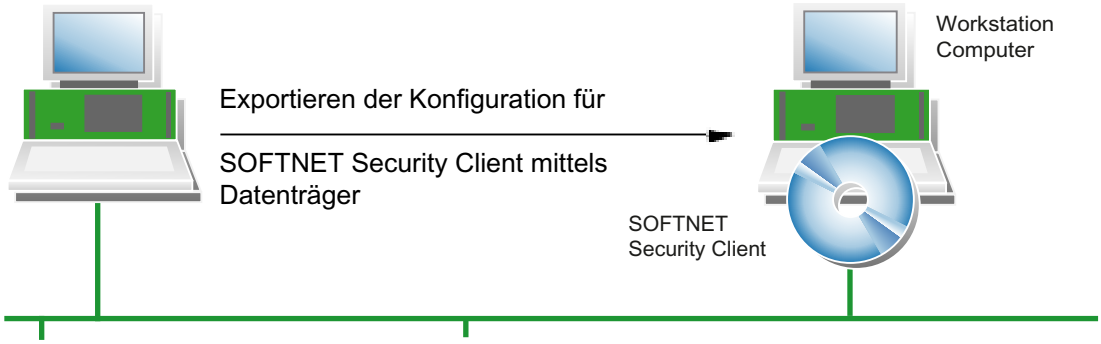
ATENCIÓN
Tenga en cuenta las indicaciones relativas a los parámetros que se describen en el capítulo 6.4, apartado "Ajustes compatibles para SOFTNET Security Client".

Nota

Si crea varios SOFTNET Security Clients dentro de un grupo, no se establece túnel alguno entre esos Clients, sino sólo entre el respectivo Client y los módulos SCALANCE S.

Archivos de configuración para SOFTNET Security Client

La interfaz entre la herramienta de configuración Security Configuration Tool y el SOFTNET Security Client es operada a través de archivos de configuración.



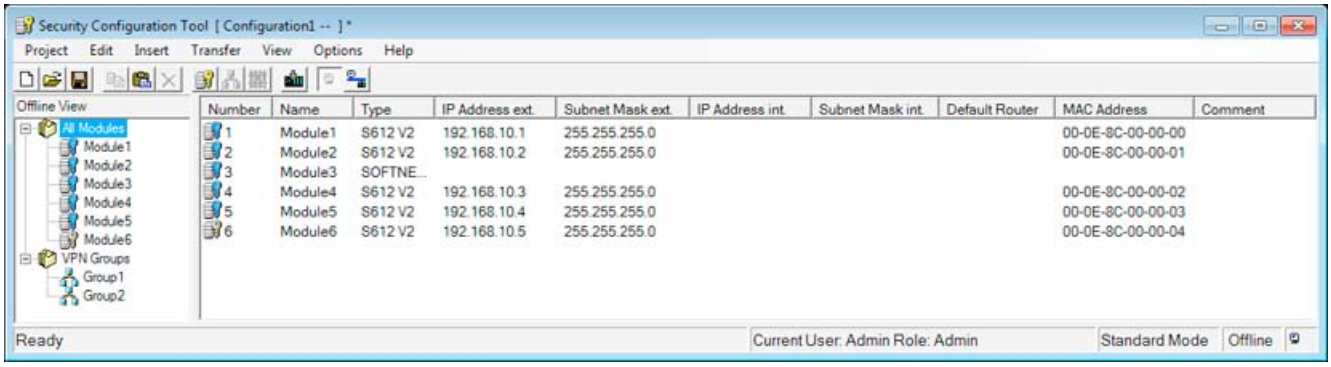
La configuración se almacena en los siguientes tres tipos de archivos:

- *.dat
- *.p12
- *.cer

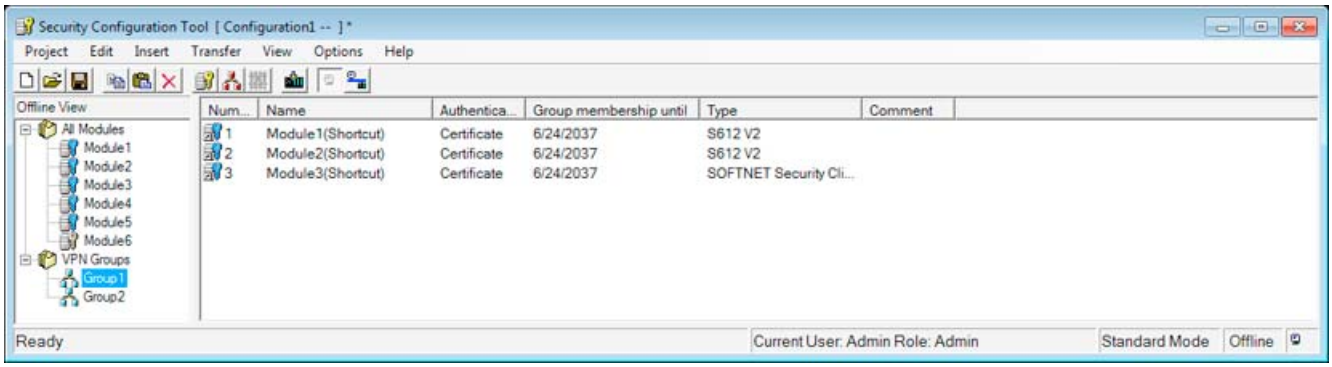
Procedimiento

Realice en la herramienta de configuración Security Configuration Tool las siguientes operaciones para crear los archivos de configuración:

1. Habilite primero en su proyecto un módulo del tipo SOFTNET Security Client.


Security Configuration Tool [Configuration1 --] *
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
Module6
VPN Groups
Group1
Group2
Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. Default Router MAC Address Comment
1 Module1 S612 V2 192.168.10.1 255.255.255.0 00-0E-8C-00-00-00
2 Module2 S612 V2 192.168.10.2 255.255.255.0 00-0E-8C-00-00-01
3 Module3 SOFTNE...
4 Module4 S612 V2 192.168.10.3 255.255.255.0 00-0E-8C-00-00-02
5 Module5 S612 V2 192.168.10.4 255.255.255.0 00-0E-8C-00-00-03
6 Module6 S612 V2 192.168.10.5 255.255.255.0 00-0E-8C-00-00-04
Ready
Current User: Admin Role: Admin
Standard Mode
Offline

2. Asigne el módulo a los grupos de módulos en los que el PC/PG se deba comunicar a través de túneles IPsec.



3. Seleccione el SOFTNET Security Client deseado con el botón derecho del ratón y seleccione a continuación el comando de menú:

   Transfer ▸ To Module...

4. Seleccione en el cuadro de diálogo presentado el lugar donde quiere almacenar el archivo de configuración.
5. Si ha elegido "Certificate" como método de autenticación, en el siguiente paso se le pedirá que introduzca una contraseña para el certificado de la configuración de VPN. Aquí tiene la posibilidad de asignar una contraseña propia. Si no asigna ninguna contraseña, se adopta el nombre del proyecto como contraseña.

   La entrada de la contraseña se realiza, como de costumbre, con repetición.

   Con esto ha concluido la exportación de los archivos de configuración.
6. Transfiera los archivos del tipo *.dat, *.p12, *.cer al PC/PG en el que desee utilizar el SOFTNET Security Client.

7.4 Operación de SOFTNET Security Client

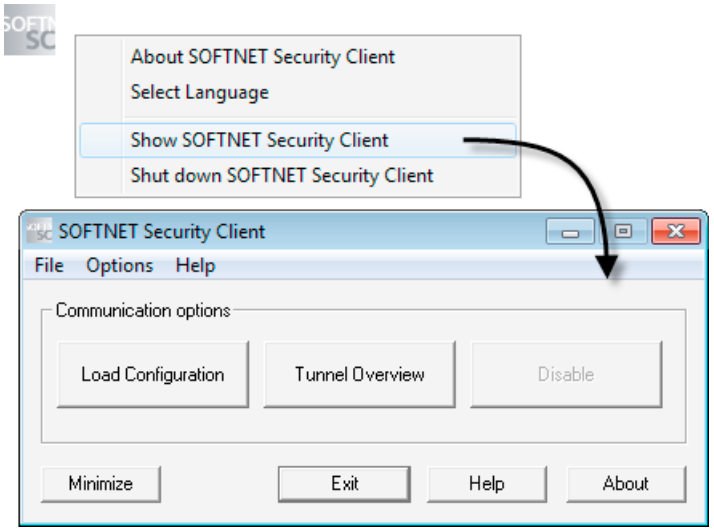
Propiedades configurables

En concreto se pueden utilizar los siguientes servicios:

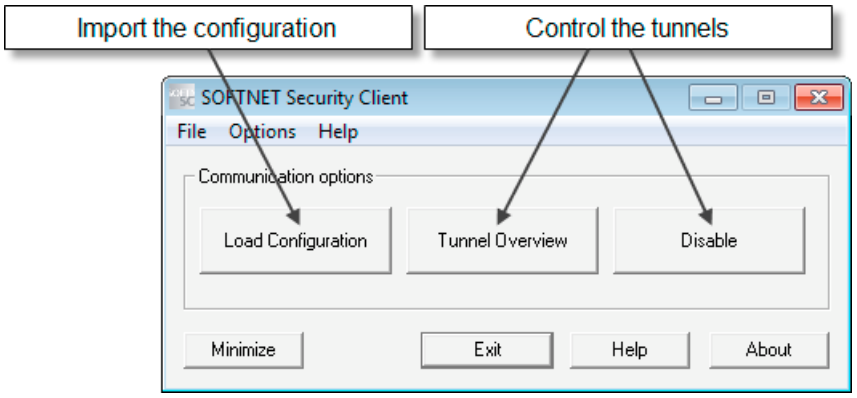
- Configuración de una comunicación segura por túnel IPsec (VPN) entre el PC/PG y todos los módulos SCALANCE S de un proyecto o módulos SCALANCE S individuales. El PC/PG puede acceder a nodos internos de la VPN a través de este túnel IPsec.
- Desactivación y activación de conexiones seguras ya configuradas.
- Configuración de conexiones en caso de equipos terminales agregados con posterioridad (para esto tiene que estar activado el modo de aprendizaje).
- Comprobación de una configuración, es decir, ver qué conexiones están habilitadas o son posibles.

Llamada de SOFTNET Security Client para la configuración

Abra la superficie de operación de SOFTNET Security Client haciendo un doble clic en el icono en SYSTRAY o seleccionando con el botón derecho del ratón el tópico de menú "Open SOFTNET Security Client":



A través de los botones se accede a las siguientes funciones:



Botón	Significado
Load Configuration Data (Cargar por lectura datos de configuración)	Importar la configuración Con esto se abre un cuadro de diálogo para la selección de un archivo de configuración. Tras cerrar el cuadro de diálogo se carga por lectura la configuración y se pregunta por una contraseña para cada archivo de configuración. En el cuadro de diálogo se pregunta si el túnel se debe establecer inmediatamente para todos los SCALANCE S. Si en la configuración están registradas direcciones IP de SCALANCE S o si está activo el modo de aprendizaje, se establecen los túneles para todas las direcciones configuradas o determinadas. Este procedimiento es particularmente rápido y eficiente para configuraciones pequeñas. Como opción, en el cuadro de diálogo de "Vista general de túneles" se pueden configurar también todos los túneles. Observación: Se pueden importar consecutivamente los archivos de configuración de varios proyectos creados en la Security Configuration Tool (vea también la explicación siguiente sobre el procedimiento).
Tunnel Overview	Cuadro de diálogo para configurar y editar túneles. A través de este cuadro de diálogo se realiza la configuración propiamente dicha del SOFTNET Security Client. En este cuadro de diálogo encontrará una lista de los túneles seguros establecidos. Allí se pueden visualizar y comprobar las direcciones IP para los módulos SCALANCE S. Si en su PG/PC existen varios adaptadores de red, el SOFTNET Security Client selecciona automáticamente uno de ellos, a través del cual se intenta establecer un túnel. Pero es posible que el SOFTNET Security Client no consiga encontrar uno apropiado para su estación, en cuyo caso introduce uno cualquiera. En tal caso tiene que adaptar manualmente la configuración de adaptadores de red a través del cuadro de diálogo "Network Adapters" en el menú contextual de la estación y del módulo SCALANCE S.
Disable	Desactivación de todos los túneles seguros. Aplicación: si se modifica o se carga de nuevo la configuración de un módulo SCALANCE S612 / S613, debería desactivar el túnel que conduce al SOFTNET Security Client. Con esto se acelera el nuevo establecimiento de túneles.
Minimize	Se cierra la interfaz de operador del SOFTNET Security Client. El icono para el SOFTNET Security Client sigue estando en la barra de tareas de Windows.
Quit	Cancelación de la configuración; se sale de SOFTNET Security Client; se desactivan todos los túneles.
Help	Llamada de la ayuda online.
Info	Información sobre la versión del SOFTNET Security Client Detalles: Lista de todos los archivos necesarios para la función del SOFTNET Security Client con notificación sobre si éstos se podrían encontrar en el sistema

7.5 Configuración y edición de túneles

Configuración de conexiones seguras con todos los SCALANCE S

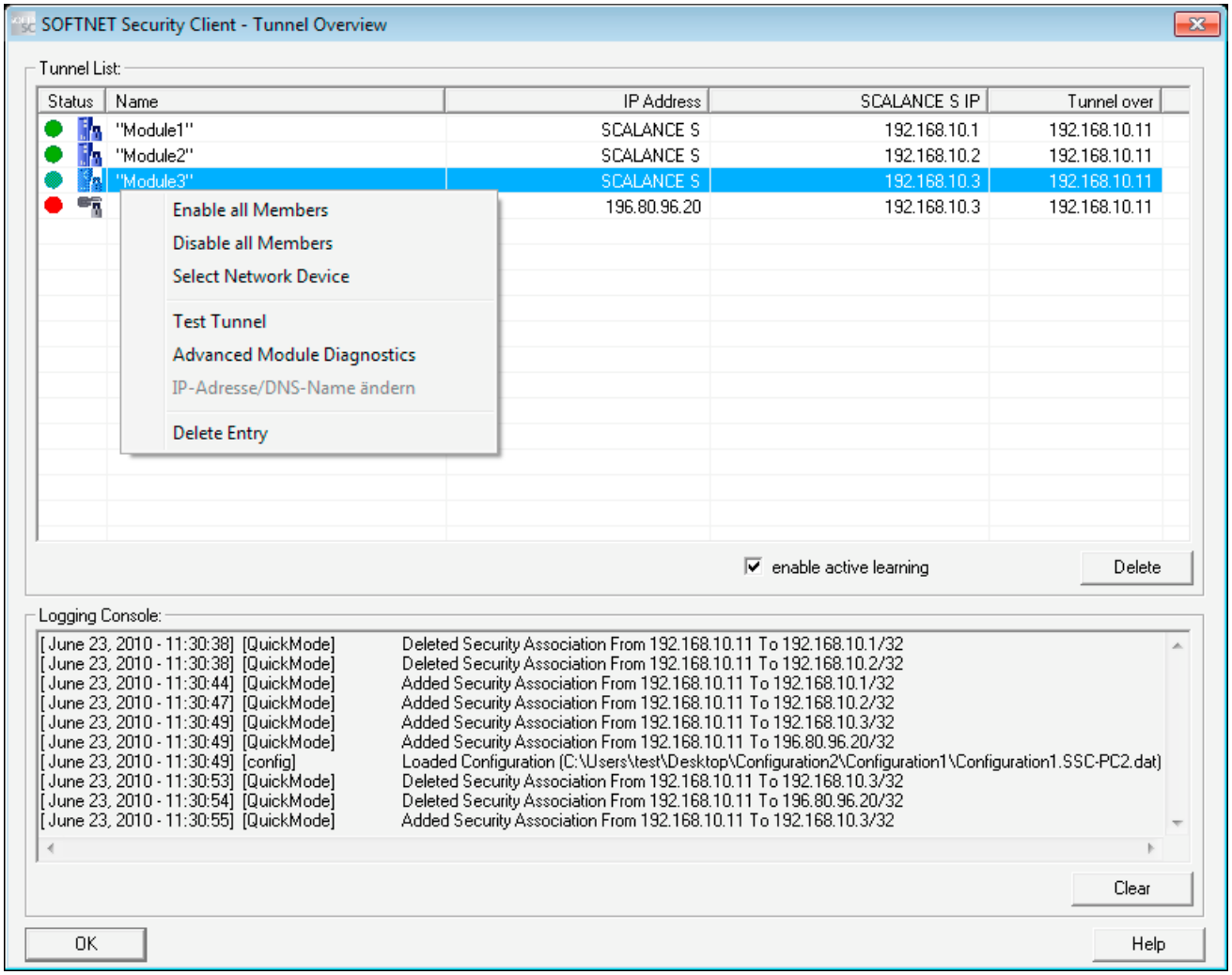
En el cuadro de diálogo para la importación de la configuración puede elegir si los túneles se deben configurar inmediatamente para todos los SCALANCE S. De esto resultan las siguientes posibilidades:

- Activación automática del túnel

  Si en la configuración están registradas direcciones IP de SCALANCE S o si está activo el modo de aprendizaje, se establecen los túneles para todas las direcciones configuradas o determinadas.

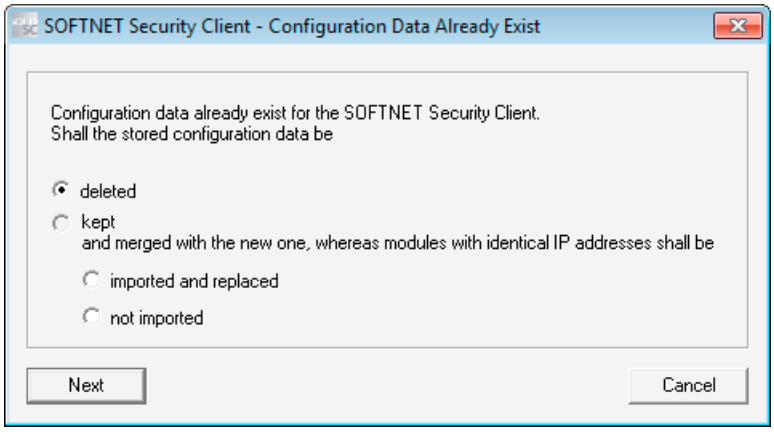
- Sólo lectura de la configuración del túnel

  Como opción se puede realizar sólo la lectura de los túneles configurados, activándolos luego individualmente en el cuadro de diálogo para la configuración de túneles.


SOFTNET Security Client - Tunnel Overview
Tunnel List:
Status
Name
IP Address
SCALANCE S IP
Tunnel over
"Module1"
SCALANCE S
192.168.10.1
192.168.10.11
"Module2"
SCALANCE S
192.168.10.2
192.168.10.11
"Module3"
SCALANCE S
192.168.10.3
192.168.10.11
196.80.96.20
192.168.10.3
192.168.10.11
Enable all Members
Disable all Members
Select Network Device
Test Tunnel
Advanced Module Diagnostics
IP-Adresse/DNS-Name ändern
Delete Entry
enable active learning
Delete
Logging Console:
[June 23, 2010 - 11:30:38] [QuickMode] Deleted Security Association From 192.168.10.11 To 192.168.10.1/32
[June 23, 2010 - 11:30:38] [QuickMode] Deleted Security Association From 192.168.10.11 To 192.168.10.2/32
[June 23, 2010 - 11:30:44] [QuickMode] Added Security Association From 192.168.10.11 To 192.168.10.1/32
[June 23, 2010 - 11:30:47] [QuickMode] Added Security Association From 192.168.10.11 To 192.168.10.2/32
[June 23, 2010 - 11:30:49] [QuickMode] Added Security Association From 192.168.10.11 To 192.168.10.3/32
[June 23, 2010 - 11:30:49] [QuickMode] Added Security Association From 192.168.10.11 To 196.80.96.20/32
[June 23, 2010 - 11:30:49] [config] Loaded Configuration (C:\Users\test\Desktop\Configuration2\Configuration1\Configuration1.SSC-PC2.dat)
[June 23, 2010 - 11:30:53] [QuickMode] Deleted Security Association From 192.168.10.11 To 192.168.10.3/32
[June 23, 2010 - 11:30:54] [QuickMode] Deleted Security Association From 192.168.10.11 To 196.80.96.20/32
[June 23, 2010 - 11:30:55] [QuickMode] Added Security Association From 192.168.10.11 To 192.168.10.3/32
Clear
OK
Help

Establecimiento de conexiones de túnel

1. Abra con el botón "Load Configuration Data" el cuadro de diálogo para importar el archivo de configuración.
2. Seleccione el archivo de configuración creado con la Security Configuration Tool.
3. Si en el SOFTNET Security Client existen ya datos de configuración, se le pide ahora que decida sobre cómo se debe proceder con los nuevos datos de configuración a adoptar. Elija entre las opciones ofrecidas:


SOFTNET Security Client - Configuration Data Already Exist
Configuration data already exist for the SOFTNET Security Client.
Shall the stored configuration data be
deleted
kept
and merged with the new one, whereas modules with identical IP addresses shall be
imported and replaced
not imported
Next
Cancel

Observaciones relativas a este cuadro de diálogo:

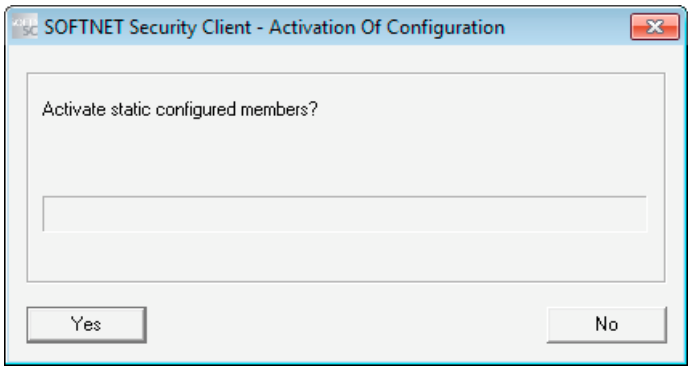
Básicamente se pueden cargar los datos de configuración de varios proyectos. Con este cuadro de diálogo se toman en consideración las condiciones generales correspondientes a varios proyectos. En consecuencia, las opciones tienen la siguiente **repercusión:**

- Con "remove" están disponibles sólo los últimos datos de configuración cargados.
- El segundo punto de selección "import and replace" es conveniente en el caso de datos de configuración modificados, por ejemplo si sólo se ha modificado la configuración en el proyecto a y se conservan inalterados los proyectos b y c.
- El tercer punto de selección "don't import" es conveniente si en un proyecto se ha agregado un SCALANCE S, sin que se pierdan nodos internos ya programados.

4. Si al configurar en la Security Configuration Tool ha seleccionado "Certificate" com método de autenticación, se le pide ahora que introduzca una contraseña.

5. Seleccione ahora si se deben activar las conexiones de túnel para las estaciones configuradas en la configuración (estaciones de configuración estática).

   Si no impulsa aquí todavía la activación, lo puede hacer en todo momento en el cuadro de diálogo para túneles que se describe a continuación.

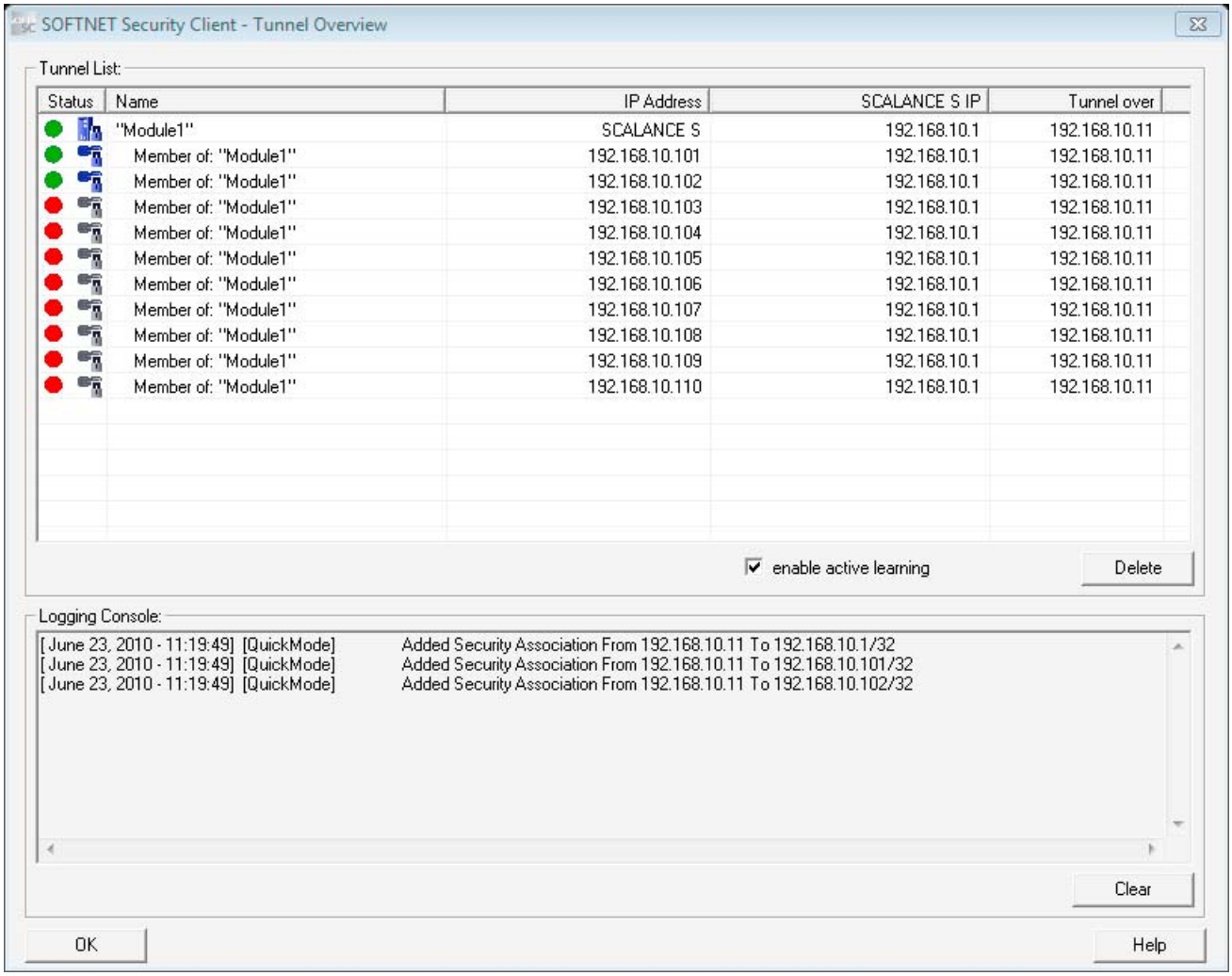


   Si ha seleccionado la activación de las conexiones de túnel, éstas se establecen ahora entre SOFTNET Security Client y los módulos SCALANCE S.

   Esto puede durar varios segundos.

6. Abra ahora el cuadro de diálogo "Tunnel Overview"

   En la tabla que se presenta puede ver los módulos y las estaciones, con informaciones sobre el estado de las conexiones de túneles.



7. Si constata ahora que no se visualizan en la tabla nodos o estaciones deseados, proceda del siguiente modo:

   Emita a través de la línea de comandos un comando PING al nodo deseado.

   Con esto hace que el nodo sea programado por el SCALANCE S y se transmita al SOFTNET Security Client.

   Observación:

   Si el cuadro de diálogo no está abierto mientras se registra una estación, se presenta automáticamente el cuadro de diálogo.

Nota

Estaciones y subredes configuradas estáticamente

Si al utilizar SCALANCE S612 / S613 tiene que configurar estaciones o subredes estáticamente, tiene que cargar también de nuevo la configuración para un SOFTNET Security Client empleado en el grupo VPN.

8. Active las estaciones para las que se indique como estado que no se ha establecido aún ninguna conexión de túnel.

   Una vez establecida con éxito la conexión puede iniciar su aplicación, por ejemplo STEP 7, y establecer una conexión de comunicación con una de las estaciones.

ATENCIÓN
Si en su PG/PC existen varios adaptadores de red, el SOFTNET Security Client selecciona automáticamente uno de ellos, a través del cual se intenta establecer un túnel. Pero es posible que el SOFTNET Security Client no consiga encontrar uno apropiado para su proyecto, en cuyo caso introduce uno cualquiera. En tal caso tiene que adaptar manualmente la configuración de adaptadores de red a través del menú contextual de la estación y del módulo SCALANCE S.

Significado de los parámetros

Tabla 7- 1 Parámetros en el cuadro de diálogo "Tunnel over:..."

Parámetros	Significado / margen de valores
Status	Encontrará indicaciones de estado posibles en la tabla 7–2
Name	Nombre del módulo o de la estación, tomado de la configuración con Security Configuration Tool.
IP participante int. / subred	Dirección IP del nodo interno, o ID de red de la subred interna si es que se dispone de participantes / subredes internos
IP de punto final de túnel	Dirección IP del módulo SCALANCE S o MD741-1 asignado
Tunnel over..	Si utiliza varias tarjetas de red en su PC, se muestra aquí la dirección IP asignada.

Tabla 7- 2 Indicaciones de estado

Icono	Significado
	No hay conexión con el módulo o la estación participante.
	Existen otras estaciones participantes que no son visualizadas. Haga un doble clic en este icono para ver más estaciones.
	La estación participante no está activada.
	La estación participante está activada.
	Módulo SCALANCE S desactivado.
	Módulo SCALANCE S activado.

Icono	Significado
	Módulo MD741-1 desactivado.
	Módulo MD741-1 activado.
	El módulo / la estación participante no es accesible.
	El módulo / la estación participante es accesible.

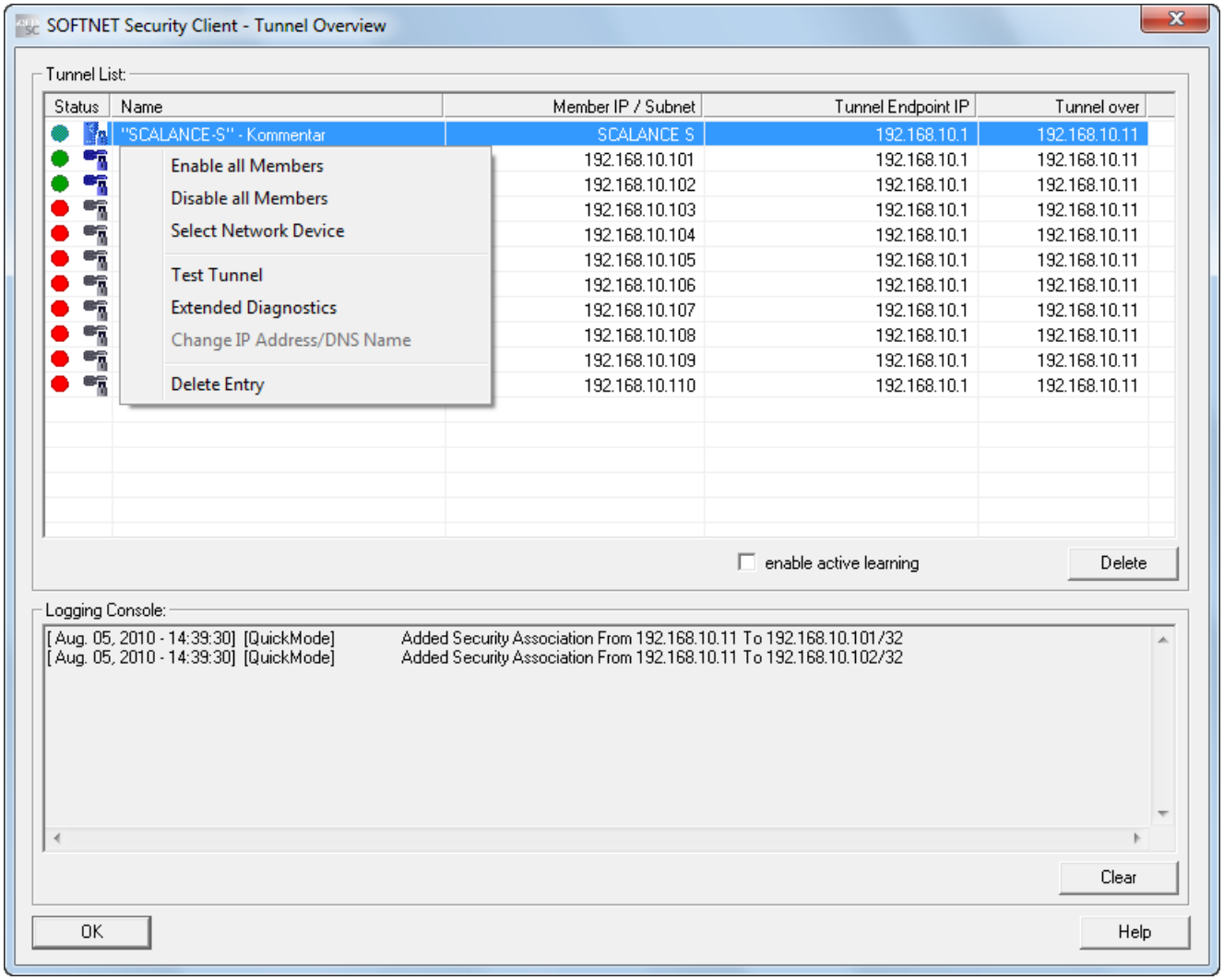
Casilla de control "enable active learning"

Si en la configuración de los módulos SCALANCE S está activado el modo de aprendizaje, puede utilizar también dicho modo para el SOFTNET Security Client; con esto obtiene autom´ticamente informaciones de los módulos SCALANCE S.

En otro caso, el campo de selección "Activate learning mode" está inactivo y aparece en gris.

Selección y operación de la entrada "túnel"

En el cuadro de diálogo "Tunnel" puede seleccionar una entrada y abrir otros comandos de menú con el botón derecho del ratón.



ATENCIÓN
Si se utilizan varias direcciones IP para un adaptador de red, es posible que tenga que asignar en el cuadro de diálogo "Tunnel" para cada una de las entradas la dirección IP a utilizar en cada caso.

Botón "Delete All"

Con él borra por completo la directiva de seguridad IP, incluidas entradas adicionales, no creadas por el SOFTNET Security Client.

Desactivación y activación de conexiones seguras ya configuradas

Conexiones seguras configuradas se pueden desactivar con el botón "Disable". Al hacer clic en el botón cambia el texto en el botón a "Connect" y se reemplaza el icono en la barra de estado.

Ahora está desactivada internamente la Security Policy en el PC.

Con un nuevo clic en el botón se puede anular la modificación anterior y vuelven a estar activos los túneles configurados.

Consola de Log

La consola de Logging se encuentra en la parte inferior del cuadro de diálogo "Tunnel Overview" y proporciona información de diagnóstico sobre el establecimiento de la conexión con los módulos SCALANCE S / MD741-1 configurados y estaciones participantes / subredes internas.

Con sellos de fecha y hora se pueden registrar los momentos en que se producen los eventos correspondientes.

Se visualiza el establecimiento y la disolución de una Security Association. Igualmente se visualiza el resultado de un ping de test (test de accesibilidad) relativo a las estaciones configuradas, si es negativo.

Puede usted configurar las salidas que se deben mostrar en el cuadro de diálogo "Ajustes".

Botón "Empty list"

Usted borra las entradas de la consola log de la vista general del túnel.

Ajustes globales para SOFTNET Security Client

Abra el punto de menú en el diálogo principal del SOFTNET Security Client:

Options ▸ Settings

Aquí puede hacer los ajustes globales que quedarán tras finalizar y abrir el SOFTNET Security Client.

Las funciones se pueden ver en la siguiente tabla.

Función	Descripción / opciones
Tamaño del archivo Log (consola log)	Tamañalo del archivo log del archivo fuente que contene los mensajes que se emiten en la consola log filtrados y limitados a una cantidad determinada.
Número de mensajes que se deben mostrar en la consola log de la vista general del túnel.	Número de mensahes que se extraen del archivo log del archivo fuente y que se muestran en la consola log.

Función	Descripción / opciones
Se emiten los siguientes mensajes log en la consola log de la vista general del túnel: • Visualización del test de accesibilidad negativo (Ping) • Crear / borrar Security Associations (Quick Modes) • Crear / borrar Main Modes • Cargar archivos de configuración • Aprendizaje de estaciones participantes internas	Los mensajes que se visualizan opcionalmente en la consola log, pueden conectarse y desconectarse aquí.
Tamaño del archivo log (Debug logfile)	Tamaño del archivo log de los archivos fuente para mensajes Debug del SOFTNET Security Client (pueden ser reclamados por el Customer Support para facilitar los análisis)
Test de accesibilidad, tiempo de espera para la respuesta	Hora de espera ajustable para el ping que debe indicar la accesibilidad de un socio del túnel. Sobre todo hay que ajustarlo en túneles a través de vías de transmisión lentas (UMTS, GPRS, etc.), en las que el tiempo de ejecución de los paquetes de datos es notablemente más largo. De esta forma se influye directamente en la visualización de la accesibilidad de la vista del túnel. **Nota** Seleccione en las redes inalámbricas un tiempo de espera de 1500 ms, como mínimo.
Desactivar globalmente el test de accesibilidad	Si usted activa esta función, se desactiva globalmente el test de accesibilidad en todas las configuraciones recibidas del SOFTNET Security Client. Este aspecto tiene la ventaja de que no se producen paquetes de volúmenes de datos adicionales, y la desventaje de que en la vista del túnel no se reciben más mensajes de respuesta sobre si el socio del túnel es accesible o no.

Diagnóstico de módulo ampliado

Abra el punto de menú en el diálogo principal del SOFTNET Security Client:

Opciones ▸ Diagnóstico de módulo ampliado

Aquí puede usted determinar el estado actual de su sistema comparándolo con un módulo configurado. Esta vista sirve íntegramente para el diagnóstico del estado de su sistema, y puede ayudar en las consultas del Customer Support.

- Módulo SCALANCE S / MD741-1
  Aquí selecciona usted el módulo para el que desea diagnosticar el estado de sistema actual.
- Ajustes de rutina (parámetros específicos de módulos)
  En este caso se le indican los ajustes del módulo determinados por la configuración teniendo en cuenta sus interfaces y nodos / subredes internos.

- Active Main Modes / Active Quick Modes
  Aquí se le muestran en detalle los Main Modes o Quick Modes activos en cuanto éstos han sido incorporados para el módulo seleccionado en el PG/PC.
  Además puede ver también cuántos Main Modes o Quick Modes se encontrarían en el sistema adecuados para el módulo seleccionado.
- Los ajustes de Routing (ajustes de red del ordenador)
  Aquí se le muestran los ajustes de Routing actuales de su ordenador.
  Con la opción "Mostrar todos los ajustes de Routing" puede usted mostar los ajustes de routing ocultos por cuestiones de mayor claridad.
- Direcciones IP asignadas
  Aquí dispone usted de una lista sobre las interfaces de red de las que dispone conocidas para el ordenador en relación con las direcciones IP configuradas o asignadas.

Funciones online - Test, Diagnóstico y Logging

8

Con fines de comprobación y supervisión se ha dotado el SCALANCE S de funciones de diagnóstico y logging.

- Funciones de diagnóstico

  Por esto se entienden diversas funciones del sistema y de estado que se pueden utilizar en el modo online.

- Funciones de logging

  Se trata al respecto del registro de eventos del sistema y relacionados con la seguridad.

Los eventos se registran en áreas búfer del SCALANCE S o de un servidor. La parametrización y la evaluación de estas funciones exigen disponer de una conexión de red para el módulo SCALANCE S seleccionado.

Registrar eventos con funciones logging

Usted define qué eventos se deben registrar por medio de los ajustes de log para el respectivo módulo SCALANCE S.

A su vez puede configurar las siguientes variantes para el registro:

- Local Log

  Con esta variante se registran los eventos en el búfer local del módulo SCALANCE S. En el diálogo online de la Security Configuration Tool puede recurrir entonces a este registro, hacerlo visible y archivarlo en la Service Station.

- Syslog de red

  En el caso de Network Syslog utiliza un servidor Syslog existente en la red. Éste registra los eventos para el respectivo módulo SCALANCE S conforme a la configuración de los ajustes de log.

Otras informaciones

Encontrará informaciones detalladas sobre los cuadros de diálogo y los parámetros registrados en el diagnóstico en el logging en la ayuda online de la Security Configuration Tool.

Puede acceder a esta ayuda con la tecla F1 o con el botón "?" en el respectivo cuadro de diálogo.

Consulte también

Panorámica de funciones del cuadro de diálogo online (Página 222)

8.1 Panorámica de funciones del cuadro de diálogo online

SCALANCE S ofrece las siguientes funciones en el cuadro de diálogo online:

Tabla 8- 1 Funciones y logging en el diagnóstico online

Función / ficha en el diálogo online	Significado
Funciones de sistema y estado	
Status	Visualización del estado del módulo SCALANCE S seleccionado en el proyecto.
Communications status (S612/ S613)	Visualización del estado de comunicación y de los nodos de red internos hacia otros de los módulos SCALANCE S pertenecientes al grupo de VPN.
Date and time	Ajuste de la fecha y la hora.
Internal nodes (S612/S613)	Visualización de los nodos de red internos del módulo SCALANCE S.
Funciones de logging	
System Log	Visualización de eventos de sistema registrados.
Audit Log	Visualización de eventos de seguridad registrados.
Packet Filter Log	Visualización de los paquetes de datos registrados, así como inicio y parada del registro de paquetes.

Observación: Tenga en cuenta las observaciones sobre los tipos de equipos.

Condiciones para el acceso

Para poder ejecutar en línea las funciones online en un módulo SCALANCE S, se tienen que cumplir los siguientes requisitos:

- está activado el modo Online en la Security Configuration Tool
- existe una conexión de red con el módulo seleccionado
- está abierto el proyecto correspondiente, con el que se ha configurado el módulo.

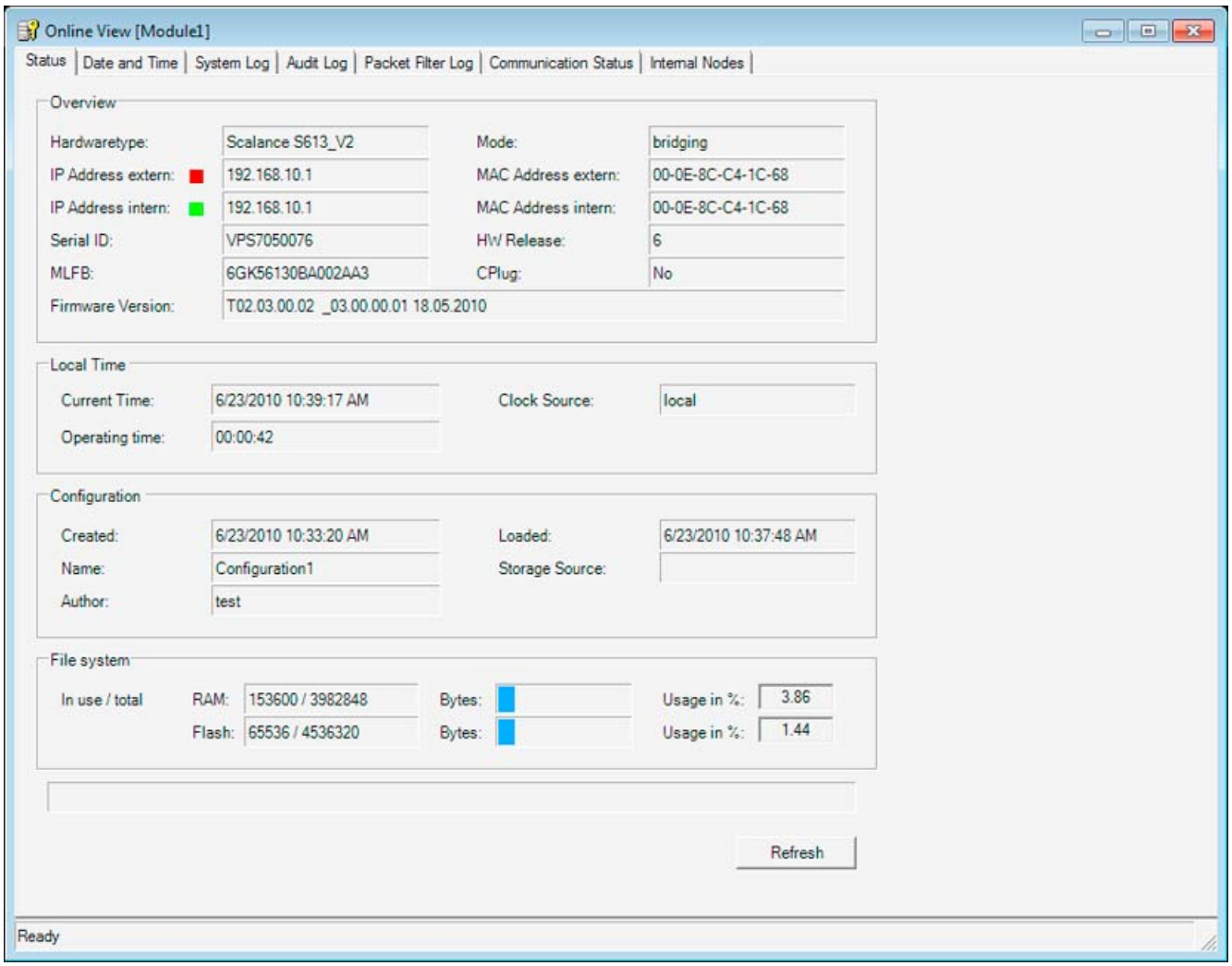
Apertura del cuadro de diálogo online

Conmute el modo de funcionamiento de la Security Configuration Tool con el comando de menú siguiente:

View ▸ Online

Marque el módulo a editar y seleccione, para abrir el cuadro de diálogo online, el comando de menú

Edit ▸ Online Diagnostics…



Advertencia en caso de una configuración no actual o de un proyecto distinto

Al llamar el diálogo online se comprueba si la configuración existente actualmente en el módulo SCALANCE S y la configuración del proyecto cargado coinciden. Si estas configuraciones difieren, se emite un mensaje de advertencia. Con esto se señaliza que usted no ha actualizado (todavía) la configuración o bien que utiliza un proyecto equivocado.

Ajustes online no se almacenan en la configuración

Los ajustes realizados en el modo online no se almacenan en la configuración del módulo SCALANCE S. Tras un rearranque del módulo actúan por ello siempre los ajustes almacenados en la configuración.

8.2 Registro de eventos (Logging)

Resumen

Se pueden registrar eventos producidos en el SCALANCE S. El registro se realiza en áreas de memoria búfer locales volátiles o permanentes, según el tipo de evento. Como alternativa puede tener lugar también el registro en un servidor de red.

Configuración en Standard y Advanced Mode

Las posibilidades de selección en la Security Configuration Tool dependen, también para el logging, de la vista seleccionada:

- Standard Mode

  Local Log está activado como opción predeterminada en el Standard Mode; los eventos de filtro de paquetes se pueden activar globalmente en la ficha "Firewall". Network Syslog no es posible en esta vista.

- Advanced Mode

  Se pueden activar o desactivar directamente todas las funciones de logging; los eventos de filtro de paquetes se tienen que activar selectivamente en la ficha "Firewall" (reglas locales o globales).

Métodos de registro y clases de eventos

Puede definir en la configuración qué datos se deben registrar. De este modo activa ya el registro al cargar la configuración en el módulo SCALANCE S.

Además elige en la configuración uno de los métodos de registro o ambos:

- Local Log
- Network Syslog

El SCALANCE S reconoce para cada método de registro los tres tipos de eventos siguientes:

Tabla 8- 2 Logging - panorámica de eventos seleccionables

Función / ficha en el diálogo online	Funcionamiento
Packet filter events (Firewall) / Packet Filter Log	El Packet Filter Log registra determinados paquetes del tráfico de datos. Sólo se registran paquetes de datos para los que sea válida un regla de filtrado de paquetes (firewall) configurada o frente a los que reacciona la protección básica (paquetes corruptos o no válidos). Condición para ello es que esté activado el registro para la regla de filtrado de paquetes.
Audit events / Audit Log	Audit Log registra de forma automática y continua eventos relevantes para la seguridad. Por ejemplo, acciones del usuario xomo activación o desactivación del logging de paquetes o acciones para las que un usuario no se haya autenticado correctamente con su contraseña.
System events / System Log	El System Log registra de forma automática y continua eventos del sistema como p. ej. el inicio de un proceso. El registro se puede escalar en base a clases de eventos. Adicionalmente se puede configurar un diagnóstico de líneas. El diagnóstico de líneas proporciona mensajes en cuanto la cantidad de paquetes de telegramas incorrectos supera un valor límite ajustable.

Procedimiento de almacenamiento para el registro de datos en caso de logging local

El almacenamiento relacionado con el registro de datos se realiza según dos procedimientos seleccionables:

- **Ring Buffer**

Cuando se alcanza el final del búfer, el registro continúa al principio del búfer sobrescribiendo las entradas más antiguas.

- **One Shot Buffer**

El registro se detiene cuando el búfer está lleno.

Activación y desactivación del Logging

En el modo offline puede activar, a través de los ajustes de log (Log Settings), el logging local para las clases de eventos, definiendo entonces el método de almacenamiento en memoria. Estos ajustes de log se cargan en el módulo con la configuración y se activan al arrancar el SCALANCE S.

Si es necesario, también puede activar o desactivar en las funciones online el logging local para eventos de filtrado de paquetes y eventos del sistema. Con esto no se alteran los ajustes de la configuración del proyecto.

8.2.1 Log local - ajustes en la configuración

En el modo offline puede activar, a través de los ajustes de log (Log Settings), las clases de eventos, definiendo entonces el método de almacenamiento en memoria. Estos ajustes de log se cargan en el módulo con la configuración y se activan al arrancar el SCALANCE S.

Estos ajustes de Log configurados se pueden modificar, si es necesario, en las funciones online. Con esto no se alteran los ajustes de la configuración del proyecto.

Ajustes de log en el Standard Mode

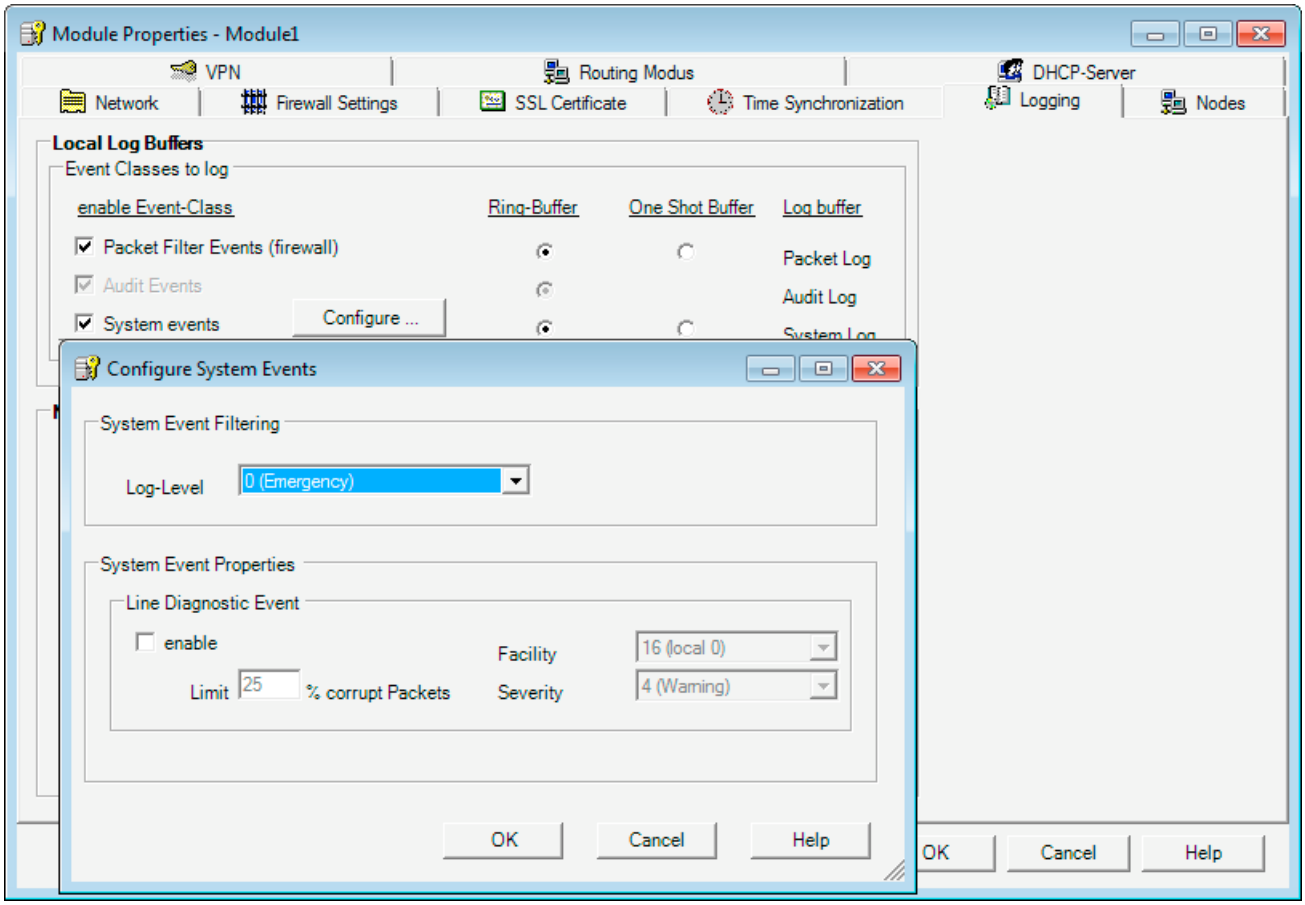
Los ajustes de log en el Standard Mode se corresponden con los preajustes en el Advanced Mode. Pero en el Standard Mode no se pueden modificar los ajustes.

Ajustes de log en el Advanced Mode

Marque el módulo a editar y seleccione el siguiente comando de menú:

Edit ▸ Properties..., ficha "Logging"

El cuadro de diálogo siguiente muestra los ajustes predeterminados para SCALANCE S; además, el cuadro de diálogo está abierto para configurar el registro de eventos del sistema:



Configuración de clases de eventos

Tabla 8- 3 Local Log - panorámica de funciones

Función / ficha en el diálogo online	Configuración	Observaciones
Packet filter events (firewall) / Packet Filter Log (configurable)	La activación tiene lugar a través de casillas de control. La selección del método de almacenamiento se realiza a través de casillas de control.	• Los datos de Packet Filter Log no son remanentes Los datos se almacenan en una memoria volátil de SCALANCE S, por lo que dejan de estar disponibles tras una desconexión de la alimentación eléctrica.
Audit events / Audit Log (siempre activado)	Logging está siempre activado. Se almacena siempre en la memoria búfer circulante.	• Los datos de Audit Log son remanentes Los datos de Audit Log se almacenan en una memoria remanente del SCALANCE S. En consecuencia, los datos de Audit Log siguen estando disponibles tras una desconexión de la alimentación eléctrica.
System events / System Log (configurable)	La activación tiene lugar a través de casillas de control. La selección del método de almacenamiento se realiza a través de casillas de control. Para configurar el filtro de eventos y el diganóstico de líneas, abra otro cuadro de diálogo con el botón "Configure...". En este subdiálogo puede ajustar un nivel de filtrado para los eventos del sistema. Está predeterminado el nivel más alto, de modo que sólo se registren eventos críticos. El diagnóstico de líneas genera un evento especial del sistema. Con ello, en caso de producirse telegramas incorrectos en un porcenteje ajustable, se genera un evento del sistema. A este evento del sistema se le asigna la prioridad y la importancia (Facility) ajustables en este subdiálogo.	• Los datos de System Log no son remanentes Los datos de System Log se almacenan en una memoria volátil del SCALANCE S. Por ello, estos datos dejan de estar disponibles tras una desconexión de la alimentación eléctrica. • Filtrado de los eventos del sistema Seleccione como nivel de filtrado "Error" o superior para impedir el registro de eventos generales, no críticos. • Prioridad de los eventos del sistema correspondientes al diagnóstico de líneas Cuide de no asignar a los eventos del sistema correspondientes al diagnóstico de líneas una prioridad menor a la ajustada para el filtro. En caso de tener una prioridad más baja, estos eventos no pasarían el filtro y no se registrarían.

8.2.2 Network Syslog - ajustes en la configuración

Puede configurar SCALANCE S de manera que envíe, como cliente Syslog, informaciones a un servidor Syslog. El servidor Syslog puede estar en la subred interna o en la externa. La implementación es conforme a RFC 3164.

Nota

Firewall - Servidor Syslog no activo en la red externa

Si el servidor Syslog no está activo en el ordenador direccionado, este ordenador devuelve, por regla general, telegramas de respuesta ICMP "port not reachable". Si debido a la configuración del firewall se registran estos telegramas de respuesta como eventos del sistema y se envían al servidor Syslog, esta operación puede continuar indefinidamente (avalancha de eventos).

Soluciones:

- Iniciar el servidor Syslog;
- Modificar reglas de firewall;
- Desconectar de la red el ordenador con el servidor Syslog desactivado;

Conmmutar al Advanced Mode

La configuración del servidor Syslog puede hacerse en la vista "Advanced Mode" de la Security Configuration Tool. Conmute el modo de funcionamiento con el siguiente comando:

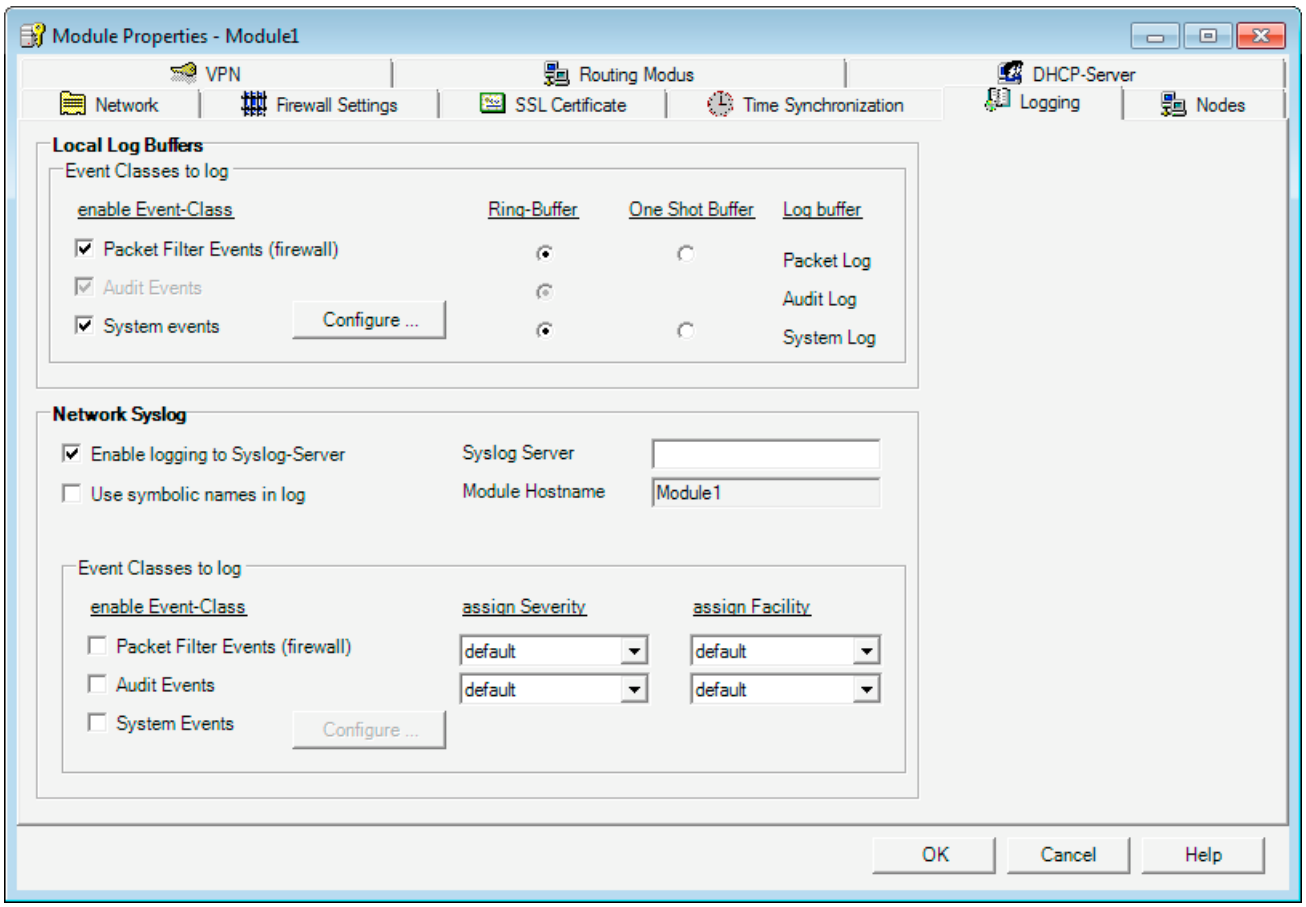
View ▸ Advanced Mode

Realizar ajustes de logging

Marque el módulo a editar y seleccione el siguiente comando de menú:

Edit ▸ Properties..., ficha "Logging"

El siguiente cuadro de diálogo le muestra la configuración estándar para SCALANCE S estando activado el logging para Network Syslog:



Establecer la conexión con el servidor Syslog

SCALANCE S utiliza el nombre de módulo configurado como nombre de host de cara al servidor Syslog. Tiene que introducir la dirección IP del servidor Syslog. Como alternativa puede introducir la dirección IP en forma de nombre simbólico o numérica.

El servidor Syslog tiene que resultar accesible desde el SCALANCE S a través de la dirección IP indicada, ajustando esto, si es necesario, a través de la configuración del router en la ficha "Network". Si no se puede acceder al servidor Syslog, se desactiva el envío de informaciones Syslog. Tal estado operativo se puede reconocer por los correspondientes mensajes del sistema. Para activar de nuevo el envío de informaciones de Syslog tendrá que actualizar eventualmente las informaciones de routing e impulsar un rearranque del SCALANCE S.

Uso de nombres simbólicos en el logging

Puede sustituir por nombres simbólicos las direcciones que aparecen en los telegramas log transmitidos al servidor Syslog. Si está activada esta opción, SCALANCE S comprueba si están configurados los nombres simbólicos correspondientes y los inscribe en los telegramas log. Tenga en cuenta que esto prolonga el tiempo de procesamiento en el módulo SCALANCE S.

Para las direcciones IP de los módulos SCALANCE S se utilizan automáticamente los nombres de los módulos como nombres simbólicos. En el modo Routing, a estos nombres se les añade una extensión con una designación de puerto: "Nombre_de _módulo-P1", "Nombre_de _módulo-P2", etc.

Configuración de clases de eventos

Tabla 8- 4 Network Syslog - panorámica de funciones

Función / ficha en el diálogo online	Configuración	Observaciones
Packet filter events (firewall) / Packet Filter Log (configurable)	La activación tiene lugar a través de casillas de control. La prioridad y la importancia (Facility) se asignan a través de listas desplegables. A cada evento se le asignan la prioridad y la importancia (Facility) aquí ajustadas.	El valor elegido para la prioridad y la importancia (Facility) dependen de la evaluación realizada en el servidor Syslog. Con esto es posible una adaptación a los requisitos del servidor Syslog. Ajustes predeterminados: Facility: 10 (security/auth) Prio: 5 (Notice)
Audit events / Audit Log (siempre activado)	La activación tiene lugar a través de casillas de control. La prioridad y la importancia (Facility) se asignan a través de listas desplegables. A cada evento se le asignan la prioridad y la importancia (Facility) aquí ajustadas.	El valor elegido para la prioridad y la importancia (Facility) dependen de la evaluación realizada en el servidor Syslog. Con esto es posible una adaptación a los requisitos del servidor Syslog. Ajustes predeterminados: Facility: 13 (log audit) Prio: 6 (Informational)
System events / System Log (configurable)	La activación tiene lugar a través de casillas de control. Para configurar el filtro de eventos y el diganóstico de líneas, abra otro cuadro de diálogo con el botón "Configure...". En este subdiálogo puede ajustar un nivel de filtrado para los eventos del sistema. Está predeterminado el nivel más alto, de modo que sólo se registren eventos críticos. El diagnóstico de líneas genera un evento especial del sistema. Con ello, en caso de producirse telegramas incorrectos en un porcenteje ajustable, se genera un evento del sistema. A este evento del sistema se le asigna la prioridad y la importancia (Facility) ajustables en este subdiálogo.	• Filtrado de los eventos del sistema Seleccione como nivel de filtrado "Error" o superior para impedir el registro de eventos generales, no críticos. • Prioridad de los eventos del sistema correspondientes al diagnóstico de líneas A través de la prioridad se valoran los eventos del sistema corresponientes al diagnóstico de líneas en relación a la prioridad de los restantes eventos del sistema. Cuide de no asignar a los eventos del sistema correspondientes al diagnóstico de líneas una prioridad menor a la ajustada para el filtro. En caso de tener una prioridad más baja, estos eventos no pasarían el filtro y no llegarían al servidor Syslog.

8.2.3 La configuración del Logging de paquetes

El Packet Filter Log registra los paquetes de datos para los que se ha activado el Logging en una regla de filtrado de paquetes (firewall) en la configuración. Por lo tanto, esta activación se tiene que configurar.

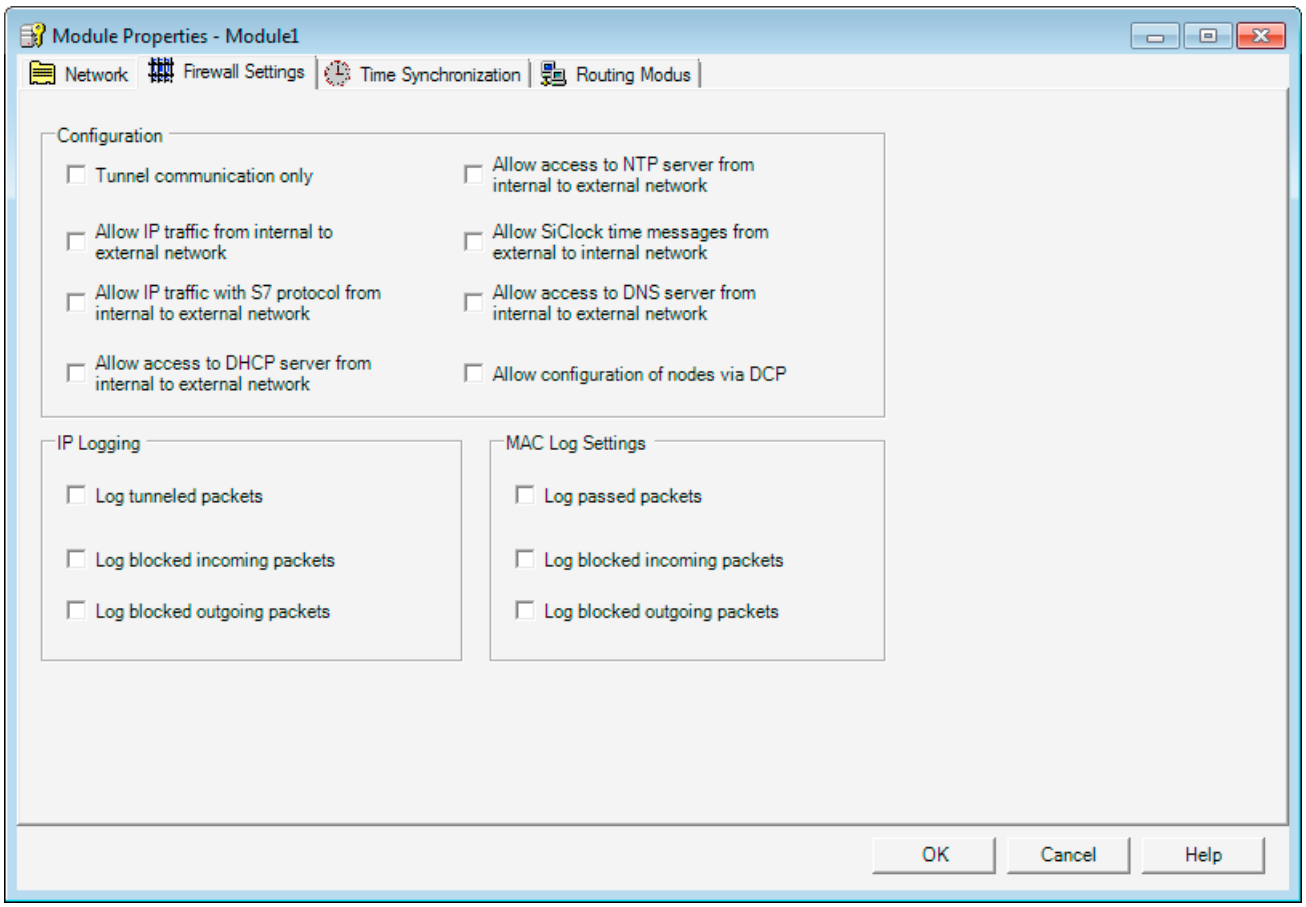
La configuración difiere dependiendo de la vista de operación ajustada. Mientras que en el Standard Mode el logging sólo se puede activar básicamente para algunos bloques de reglas predefinidos, en el Advanced Mode se puede activar para cada regla de filtrado de paquetes a nivel individual.

Configuración en el Standard Mode

En el Standard Mode existen los siguientes bloques de reglas para los ajustes de IP- y MAC-Log, para los que se puede activar el Logging:

Tabla 8- 5 Ajustes de IP y MAC Log

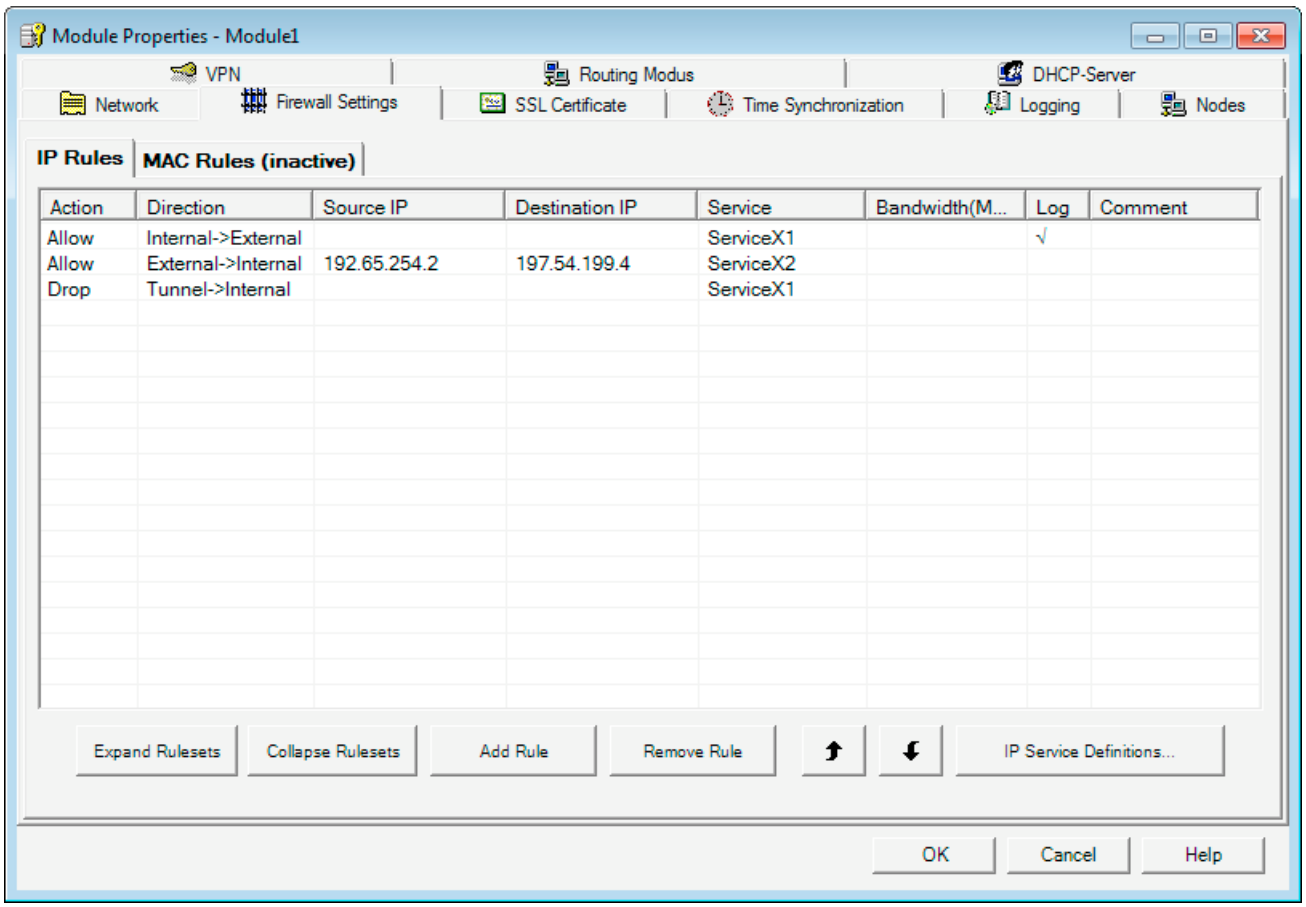
Bloque de reglas	Acción para activación
Log passed packets	Todos los paquetes MAC que se han transmitido se registran.
Log dropped incoming packets	Todos los paquetes IP / MAC entrantes que se han rechazado se registran.
Log dropped outgoing packets	Todos los paquetes IP / MAC salientes que se han rechazado se registran.
Log tunneled packets	Todos los paquetes IP que se han transmitido por el túnel se registran.


Module Properties - Module1
Network
Firewall Settings
Time Synchronization
Routing Modus
Configuration
Tunnel communication only
Allow IP traffic from internal to external network
Allow IP traffic with S7 protocol from internal to external network
Allow access to DHCP server from internal to external network
Allow access to NTP server from internal to external network
Allow SiClock time messages from external to internal network
Allow access to DNS server from internal to external network
Allow configuration of nodes via DCP
IP Logging
Log tunneled packets
Log blocked incoming packets
Log blocked outgoing packets
MAC Log Settings
Log passed packets
Log blocked incoming packets
Log blocked outgoing packets
OK
Cancel
Help

Configuración en el Advanced Mode

La activación del logging es idéntica para los dos tipos de reglas (IP o MAC) y todas las reglas.

Para registrar paquetes de datos de determinadas reglas de filtrado de paquetes, ponga una marca de selección en la columna "Log" de la ficha "Firewall".


Module Properties - Module1
VPN
Routing Modus
DHCP-Server
Network
Firewall Settings
SSL Certificate
Time Synchronization
Logging
Nodes
IP Rules
MAC Rules (inactive)
Action
Direction
Source IP
Destination IP
Service
Bandwidth(M...
Log
Comment
Allow
Internal->External
ServiceX1
√
Allow
External->Internal
192.65.254.2
197.54.199.4
ServiceX2
Drop
Tunnel->Internal
ServiceX1
Expand Rulesets
Collapse Rulesets
Add Rule
Remove Rule
IP Service Definitions...
OK
Cancel
Help

Consejos y ayuda

A

A.1 El módulo SCALANCE S no se inicializa correctamente

Si el indicador Fault del módulo SCALANCE S brilla con luz roja tras la inicialización del módulo, debería reponer en un principio el módulo por completo al estado inicial. Presione el pulsador Reset hasta que el indicador Fault comience a parpadear con luz amarilla-roja. El módulo se ha repuesto entonces a la configuración de fábrica. Para el funcionamiento productivo tiene que cargar a continuación de nuevo la configuración en el módulo.

Si el indicador Fault del módulo SCALANCE S sigue encendido, sin embargo, con luz roja, el módulo sólo podrá ser reparado en fábrica.

A.2 Módulo SCALANCE S no accesible

Si no se puede acceder al módulo SCALANCE S, compruebe u observe los siguientes puntos:

- ¿Está su ordenador en la misma red que el módulo?
- El reset de un módulo puede requerir hasta varios minutos.

A.3 Sustitución de un módulo SCALANCE S

La sustitución de un módulo SCALANCE S se puede efectuar sin PC (sin tener que cargar la configuración en el nuevo módulo). El C-PLUG del módulo a sustituir se enchufa simplemente en el nuevo módulo que se debe poner en servicio.

ATENCIÓN
¡Enchufar y desenchufar el C-PLUG únicamente en estado sin tensión!

A.4 El módulo SCALANCE S está comprometido

Un módulo SCALANCE S está comprometido si se ha revelado

- la clave privada perteneciente al certificado del server,
- la clave privada de la CA o
- la contraseña de un usuario.

Se conoce la clave privada del certificado del server

Si se ha revelado la clave privada perteneciente al certificado del server, se tiene que sustituir el certificado del server en el módulo SCALANCE S. Los nombres de usuario almacenados en el módulo SCALANCE S no se tienen que modificar en este caso.

Proceda del siguiente modo:

1. Marque el módulo a editar y seleccione el comando de menú:

   Edit ▸ Properties..., ficha "Certificate"

2. Genere un nuevo certificado.
3. Cargue la configuración en el módulo SCALANCE S.

Se conoce la clave privada de la CA

Si se ha revelado la clave privada de la CA, se tiene que sustituir el certificado de la CA en el módulo SCALANCE S. Los nombres de usuario se pueden dejar inalterados. Sin embargo, los usuarios necesitan nuevos certificados extendidos por la nueva CA.

Proceda del siguiente modo:

1. Marque el grupo a editar y seleccione el comando de menú:

   Edit ▸ Properties....

2. Genere un nuevo certificado.
3. Cargue la configuración en todos los módulos SCALANCE S pertenecientes al grupo.

Se conoce la contraseña de un usuario perteneciente al grupo de User

Si se ha revelado la contraseña de un usuario perteneciente al grupo de User, se tiene que cambiar la contraseña de ese usuario.

Se conoce la contraseña de un usuario perteneciente al grupo de Administrator

Si se trata de un usuario perteneciente al grupo de Administrator, se debería modificar también el certificado de servidor del módulo SCALANCE S.

A.5 Clave de los datos de configuración comprometida o perdida

Clave comprometida

Si se ha comprometido una clave privada de los datos de configuración del módulo SCALANCE S, se tiene que modificar la clave a través de la herramienta de configuración del módulo SCALANCE S.

Pérdida de la clave

Si se pierde la clave privada que autoriza a acceder a los datos de configuración, ya no es posible acceder al módulo SCALANCE S con la herramienta de configuración. La única posibilidad de volver a tener acceso consiste en borrar los datos de configuración, y con ello también la clave. El borrado se puede activar presionando el pulsador de Reset. Después de esto se tiene que volver a poner en servicio el módulo SCALANCE S.

A.6 Comportamiento operativo general

Adaptación de la MTU (Maximum Transmission Unit)

La MTU fija el tamaño admisible de un paquete de datos para la transmisión en la red. Si esos paquetes de datos son transmitidos entonces por SCALANCE S a través del túnel IPsec, el paquete de datos original aumenta al agregarle las informaciones de cabecera y eventualmente se tendrá que segmentar para continuar su transmisión. Esto depende de las predeterminaciones de la MTU en la red conectada. Pero una segmentación eventualmente necesaria puede causar pérdidas apreciables de rendimiento o la cancelación de la transmisión de datos.

Esto se puede evitar adaptando el formato de MTU, es decir, reduciéndolo de forma que los paquetes de datos que llegan al SCALANCE S se puedan complementar con la información adicional necesaria, sin que por ello se requiera una subsiguiente segmentación. Un tamaño razonable está en el intervalo entre 1000 y 1400 Byte.

Informaciones sobre la identificación CE

B

Designación del producto

SIMATIC NET	SCALANCE S602	6GK5602-0BA00-2AA3
SIMATIC NET	SCALANCE S612	6GK5612-0BA00-2AA3
SIMATIC NET	SCALANCE S613	6GK5613-0BA00-2AA3

Directiva sobre compatibilidad electromagnética

Directiva 89/336/CEE "Compatibilidad electromagnética"

Campo de aplicaciones

El producto está concebido para usos industriales:

Campo de aplicaciones	Requisitos relativos a	
	Emisión de interferencias	Inmunidad a interferencias
Uso industrial	EN 61000-6-4 : 2001	EN 61000-6-2 : 2001

Observar las directivas para el montaje

El producto cumple los requisitos si para la instalación y el uso se tienen en cuenta las directivas de montaje y las consignas de seguridad que aparecen en esta descripción así como en el manual "SIMATIC NET Industrial Ethernet - Redes Twisted Pair y Fiber Optic /1/".

Declaración de conformidad

Según exigen las directivas CE arriba mencionadas, la declaración de conformidad CE está a disposición de las autoridades competentes en:

Siemens Aktiengesellschaft
Bereich Automatisierungs- und Antriebstechnik
Industrielle Kommunikation (A&D SC IC)
Postfach 4848
D-90327 Nürnberg

Informaciones para fabricantes de máquinas

El producto no es una máquina en el sentido de la directiva de la CE sobre máquinas. Por esta razón no existe para este producto declaración de conformidad según la directiva de la CE sobre máquinas 89/392/CEE.

Si el producto forma parte del equipamiento de una máquina, el fabricante de la máquina lo ha de tener en cuenta en el procedimiento de declaración de conformidad.

Bibliografía

C

/1/

SIMATIC NET Industrial Twisted Pair- and Fiber Optic Netze, edición 05/2001

Núm. de referencia:
6GK1970-1BA10-0AA0 alemán
6GK1970-1BA10-0AA1 inglés
6GK1970-1BA10-0AA2 francés
6GK1970-1BA10-0AA4 italiano

/2/

El manual del sistema de módem GPRS/GSM SINAUT MD740-1 está disponible a través de:

http://support.automation.siemens.com/WW/view/de/23940893

Esquema acotado

D

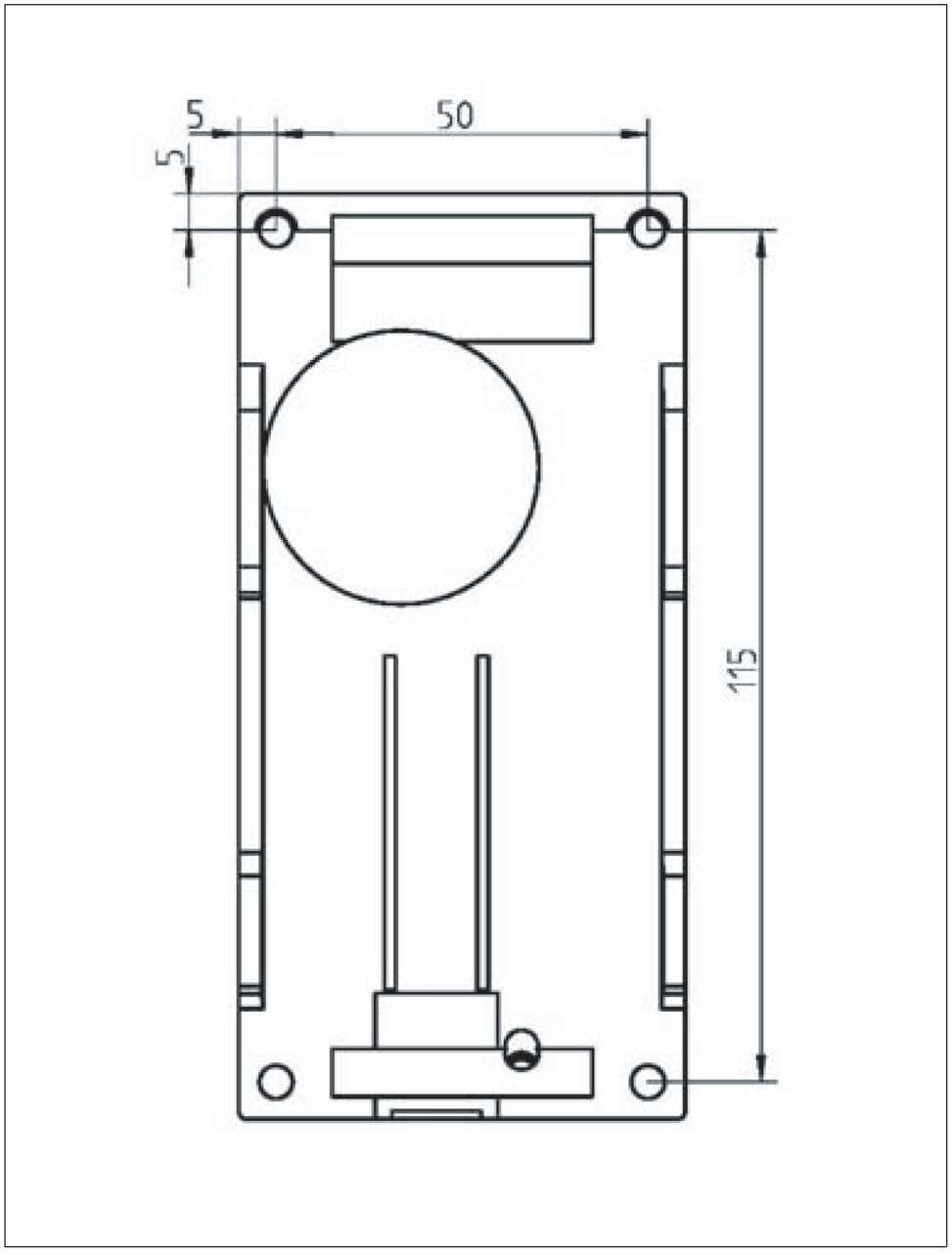


Figura D-1 Plantilla para taladrar

Historia del documento

E

E.1 Historia del documento

Esto era nuevo en la edición 02 de este manual

- **Nuevo módulo SCALANCE S602**

  Con SCALANCE S602 se dispone de otro módulo en la gama de funcionalidades de seguridad escalables. SCALANCE S602 protege con Stateful Inspection Firewall, NAT/NAPT-Routing, DHCP-Server y Syslog.

Esto era nuevo en la edición 03 de este manual

- **Modo Routing en SCALANCE S612 / S613**

  Los módulos SCALANCE S612 y S613 están disponibles con funcionalidades ampliadas; ahora se da soporte adicionalmente a NAT/NAPT-Routing, DHCP-Server y Syslog.

- **Security Configuration Tool V2.1**

  Con la nueva versión de la herramienta de configuración puede configurar los módulos S612 / S613 con sus nuevas funciones.

- **Datos de configuración para MD 740-1**

  Para configurar un MD 740-1 externo, puede crear datos de configuración con la nueva versión de la Security Configuration Tool.

Esto era nuevo en la edición 04 de este manual

- No se ha publicado la versión -

Esto era novedad en la edición 05 de este manual

En esta edición se han considerado, entre otras cosas, las siguientes nuevas funciones:

- **Security Configuration Tool V2.2**

  Se puede configurar un SOFTNET Security Client junto con un SCALANCE S en el modo Routing. (GETTING STARTED Ejemplo – Acceso remoto)

  Además d ela subred interna directa conectada al SCALANCE S, en el modo Routing se pueden configurar otras subredes, con lo que es posible acceder a las mismas.

- **SOFTNET Security Client V2.0**

  En la vista general de túneles ("Tunnel Overview") se ha añadido un campo de texto con información de diagnóstico para el establecimiento de conexiones.

  El ajuste de adaptadores de red se ha simplificado con un automatismo. En el inicio, el SOFTNET Security Client intenta encontrar automáticamente un ajuste de adaptador de red apropiado.

- **Datos de configuración para el módulo Modul MD 741-1**

  Para configurar un MD 741-1 externo, puede crear datos de configuración con la nueva versión de la Security Configuration Tool.

Esto era nuevo en la edición 06 de este manual

- **SOFTNET Security Client V3.0**

  Además de los sistemas operativos Windows XP SP2 y Windows XP SP3, también se soporta el sistema operativo Windows 7 (no la versión Home).

Glosario / lista de abreviaturas

AAA

AAA representa la síntesis de un concepto de seguridad que incluye los términos Authentication, Autorization y Accounting.

AES

Advanced Encryption Standard

Un cifrado de bloque simétrico. Se puede seleccionar en SCALANCE S para codificar los datos.

Ancho de banda

Caudal de tráfico máximo de una línea de conexión (se expresa normalmente en bps).

ARP

Address Resolution Protocol

Protocolo que sirve para la resolución de direcciones. Su tarea es encontrar para una dirección de protocolo dada la correspondiente dirección de hardware de red (dirección MAC). En hosts en los que se utiliza la familia de protocolos de Internet se encuentra también con frecuencia una implementación del protocolo ARP. A través de IP se forma una red virtual con ayuda de las direcciones IP. Éstas se tienen que representar, para el transporte de datos, en las direcciones de hardware dadas. Para realizar esta representación se utiliza con frecuencia el protocolo ARP.

BDC

Backup Domain Controller

Los Backup Domain Controller mantienen una copia de seguridad de los datos de usuario y entrada al sistema, que se actualiza a intervalos regulares.

BRI

Basic Rate Interface

Conexión de red estándar para la RDSI (ISDN).

Broadcast de subred ICMP

Para encontrar los nodos IP en la red interna, el SCALANCE S envía una ICMP-Echo-Request con la dirección Broadcast de subred IP, es decir, una dirección que accede a todos los nodos IP de la subred interna del SCALANCE S.

CA

Certification Authority

Organización para la autenticación así como la encriptación y desencriptación de datos confidenciales difundidos vía Internet y otras redes, emitiendo por ejemplo certificados digitales y firmándolos.

Certificado CA

Una autoridad de certificación (en inglés Certificate Authority, abreviado CA) es una organización que expide certificados digitales. Para la comunicación en redes informáticas, un certificado digital es el equivalente a un documento de identidad. Una autoridad de certificación otorga certificados a las estaciones de una red y los autentica.

Con SCALANCE S se genera siempre un certificado CA por cada grupo. El grupo otorga certificados a los miembros del grupo y los autentica con el certificado de grupo (certificado de grupo = certificado CA).

Certificado SSL

Se recurre a los certificados SSL para autenticar la comunicación entre

PG/PC y SCALANCE S al cargar la configuración y en el registro (logging).

CHAP

Challenge Handshake Authentication Protocol

Protocolo de autenticación utilizado en el marco del protocolo punto a punto (Point-to-Point Protocol, PPP). PPP está ubicado en la capa de seguridad de la familia de protocolos de Internet.

Client

Se entiende por Client (cliente) un equipo, o en general un objeto, que pide a un -> Server (servidor) que preste un servicio.

Conexión SSL

El protocolo SSL está asentado entre el TCP (OSI-Layer 4) y los servicios de transmisión (como p. ej. HTTP, FTP, IMAP, etc.) y sirve para una transacción protegida. SSL cuida al respecto de que el usuario se conecte inequívocamente con el servidor deseado (autenticación) y de que los datos sensibles se transmitan a través de una conexión segura (cifrada).

Convenio de codificación Diffie-Hellmann

Procedimiento para el intercambio seguro de claves secretas a través de una línea insegura.

CTRL

El campo Control (CTRL) contiene información de control para el protocolo LLC. Logical Link Control (LLC) es la denominación de un protocolo de red estandarizado por IEEE. Se trata de un protocolo cuya finalidad principal es la protección de los datos al nivel de conexiones, por lo que pertenece al nivel 2 del modelo OSI.

Data Encryption Standard

Método de encriptación de datos (encriptación de 56 bits)

DCP

Discovery and Basic Configuration Protocol.

Protocolo apropiado para determinar parámetros de direcciones de componentes PROFINET.

DES

Data Encryption Standard

Algoritmo de encriptación simétrico

DES3

Data Encryption Standard

Procedimiento simétrico de codificación, lo que significa que se utiliza la misma clave para cifrar y descifrar los datos. DES3 significa que el algoritmo se aplica tres veces, para incrementar la seguridad.

DHCP

Dynamic Host Configuration Protocol

Puede utilizar SCALANCE S como DHCP-Server en la red interna. Esto permite asignar automáticamente direcciones IP a los equipos conectados a la red interna. Las direcciones se asignan en este caso dinámicamente, desde una banda de direcciones definida por usted, o bien se asigna una dirección IP a un equipo concreto conforme a sus predeterminaciones.

DMZ

Demilitarized Zone

Red informática con posibilidades de acceso controladas seguras a los servidores a ella conectados.

Encapsulating Security Payload

Protocolo para la transmisión segura de datos

ESP

Encapsulating Security Payload

El protocolo ESP asegura que los datos transmitidos sean auténticos, íntegros y confidenciales. Con ESP es posible también comprobar sólo la autenticidad de los datos o sólo codificar datos. En el caso de SCALANCE S se emplea siempre el ESP con comprobación de la autenticidad y codificación.

Formato PKCS#12

Este estándar define un formato PKCS apropiado para el intercambio de la clave pública así como, adicionalmente, de la clave privada protegida por contraseña.

Función MDI /MDI-X Autocrossing

La función MDI /MDI-X Autocrossing ofrece la ventaja de un cableado continuo, sin que se requieran cables Ethernet externos, cruzados. Con esto se evitan funciones incorrectas por confusión de los cables de envío y recepción. La instalación se simplifica así notablemente para el usuario.

Grupos Diffie-Hellmann

Algoritmos criptográficos seleccionables en el protocolo de cambio de claves Oakley.

HTTPS

Secure Hypertext Transfer Protocol o HyperText Transfer Protocol Secured Socket Layer (SSL)

Protocolo para transmisión de datos codificados. Extensión de HTTP para la transmisión protegida de datos de carácter confidencial con ayuda de SSL.

ICMP

Internet Control Message Protocol

Protocolo auxiliar de la familia de protocolos IP, basado en el protocolo IP. Sirve para el intercambio de mensajes relativos a informaciones y errores.

ICMP-Echo-Request

Paquete Ping saliente para la verificación de la accesibilidad de un usuario de la red.

Identity-Protection

La diferencia entre la modalidad Main y Aggressive es la "Identity-Protection" que se utiliza en el Main Mode. La identidad se transmite codificada en el Main Mode, en el Aggressive Mode no.

IKE

Internet Key Exchange

Protocolo para la administración automática de claves para IPsec. IKE trabaja en dos fases. En la primera fase se autentican las dos estaciones que se comunican entre sí de forma protegida. La autenticación puede tener lugar por medio de certificados o mediante claves intercambiadas previamente (Pre Shared Keys). En la segunda fase se intercambian las claves para la comunicación de datos y se seleccionan los algoritmos de codificación.

Internet Key Exchange (IKE)

Protocolo para establecer el túnel IPsec. Aquí puede ajustar parámetros para el protocolo de la gestión de claves de IPsec. El cambio de clave tiene lugar por medio del procedimiento estandarizado IKE. (Ajustes IKE)

IP Subnet ID

ID de la subred: En base al ID de la subred, el router reconoce si una dirección de destino está en la subred o fuera de la misma.

IP/MAC Service Definition

Con ayuda de definiciones de servicios IP se pueden definir reglas de firewall de forma compacta y clara. Para esto se adjudica un nombre y se asignan al mismo los parámetros de servicio.

Además, los servicios así definidos se pueden reunir a su vez en grupos, con un nombre de grupo. Para la configuración de las reglas de filtrado de paquetes se utiliza entonces simplemente ese nombre.

ISAKMP

Internet Security Association and Key Management Protocol

Protocolo para establecer Security Associations (SA) y para el intercambio de claves criptográficas en Internet.

ISP

Internet Service Provider

Proveedor de servicios de Internet

L2F

Layer 2 Forwarding

Protocolo de red (similar a PPTP) compatible con diversos protocolos y varios túneles independientes.

L2TP

Layer 2 Tunneling Protocol

Protocolo de red que establece túneles para tramas de protocolos de la capa de seguridad (capa 2) del modelo OSI entre dos redes vía Internet para crear una red privada virtual (VPN).

Logging

Se pueden registrar eventos. El registro tiene lugar en así llamados Log (denominados de forma abreviada Log). Puede fijar ya en la configuración qué datos se deben registrar y si el registro se debe activar ya con la carga de la configuración.

Marcado VLAN

Un paquete Ethernet tiene una marca VLAN si el campo EtherType del encabezamiento del paquete Ethernet tiene un valor determinado. El encabezamiento del paquete Ethernet contiene en ese caso información sobre LAN virtuales y, eventualmente, también una prioridad de paquete.

Maximum Transmission Unit

MTU

Define el tamaño admisible de un paquete de datos para su transmisión por la red.

MD

Message Digest

Designa un grupo de protocolos criptográficos.

MD5

Message Digest Version 5

Una función criptográfica de hash muy difundida. MD5 es empleada por un gran número de aplicaciones de seguridad para verificar la integridad de los datos. En el SCALANCE S se puede seleccionar MD5 para comprobar la integridad de los datos transmitidos por un túnel.

NAPT

Network Address Port Translation

Un procedimiento en el que en un Router se reemplaza una dirección IP por otra dirección IP y adicionalmente se reemplaza el múmero de puerto por otro número de puerto en un telegrama.

NAT

Network Address Translation

Un procedimiento en el que en un Router se reemplaza por otra una dirección IP en un telegrama.

NAT-Traversal

Se trata de un método con el que se permite a los datos IPsec pasar por equipos NAT.

Nodos de red ISO

Nodos de red que no sean aptos para IP, pero que se puedan interrogar a través de protocolo ISO.

One Shot Buffer

El registro se detiene cuando el búfer está lleno.

Organizationally Unique Identifier

Designa los tres primeros bytes de la dirección MAC = identificación del fabricante.

OUI

Organizationally Unique Identifier

Cifra de 24 bits que es asignada a empresas por la IEEE Registration Authority. Las empresas usan la OUI para diversos productos de hardware, entre otras cosas como los primeros 24 bits de la dirección MAC.

PAP

Password Authentication Protocol

Protocolo de autenticación de contraseña

PEM

Privacy Enhanced Mail

Es un estándar para la encriptación de e-mails en Internet

Perfect Forward Secrecy

Perfect Forward Secrecy

Asegura que nuevas negociaciones de claves no estén en conexión con claves anteriores. La desactivación de esta opción hace posible una codificación más rápida, pero menos segura.

PGP

Pretty Good Privacy

Es un programa para la encriptación y la firma de datos.

Ping

Designación de un protocolo de test de la familia de protocolos IP. Este protocolo se encuentra presente en todo ordenador que trabaje con MS-Windows, bajo el mismo nombre, como aplicación de consola (a nivel de línea de comandos). Con "Ping" de puede pedir una respuesta (señal de vida) a un nodo de red IP dentro del conjunto de redes, siempre y cuando se conozca su dirección IP. De este modo se puede constatar si ese nodo de red está accesible a nivel de IP, verificándose así la operatividad de las funciones de SCALANCE S configuradas.

PKCS

Public Key Cryptography Standards

Son especificaciones para claves criptográficas, desarrolladas por RSA Security y otros. Un certificado vincula datos de una clave criptográfica (o de una pareja de claves, formada por clave pública y clave privada) con datos del propietario y de una entidad certificadora.

PKI

Public Key Infrastructure

En la criptología, designa un sistema que permite extender, distribuir y comprobar certificados digitales. Los certificados extendidos dentro de un PKI se utilizan para asegurar la comunicación asistida por ordenador.

PoP

Point of Presence

Noto de acceso de un proveedor de Internet

PPP

Point-to-Point Protocol - Protocolo punto a punto

PPTP

Point-to-Point Tunneling Protocol

Es un protocolo para la creación de una red privada virtual (Virtual Private Network, VPN). Permite el 'tunneling' del PPP por una red IP

Preshared Keys

Designa un procedimiento simétrico de claves. La clave se ha de dar a conocer a ambas partes antes de la comunicación. Esta clave se genera también automáticamente al crear un grupo. Sin embargo, previamente se tiene que haber introducido en el diálogo "Group Properties" de la Security Configuration Tool, en el campo "Key", una contraseña a partir de la cual se genera esta clave.

Procedimiento Public Key

El sentido de los procedimientos de codificación con clave pública es evitar por completo el riesgo para la seguridad al intercambiar mutuamente claves. Cada cual tiene una pareja de claves, con una clave pública y una secreta. Para la codificación de un mensaje se utiliza la clave pública del destinatario, y sólo éste puede volver a descifrarlo con su clave secreta.

Protocolo de intercambio de claves Oakley

El OAKLEY Key Determination Protocol describe la generación de material de codificación secreto. Forma parte del Internet-Key-Exchange-Protocols (IKE).

Protocolo MAC

Control de acceso a un medio de transmisión

PST(-Tool)

Primary Setup Tool

Con la herramienta Primary Setup Tool (PST) se pueden asignar direcciones (p. ej. la dirección IP) a componentes de red SIMATIC NET, CPs SIMATIC NET Ethernet y pasos de red.

PSTN

Public Switched Telephone Network

Sistema de comunicaciones público para la transmisión de voz entre abonados alejados.

RAS

Remote-Access Service

Con el Remote Access Service se tiene la posibilidad de conectar clientes con la red local a través de enlaces de módem, RDSI (ISDN) o X.25. En este caso no sólo se da soporte a diferentes clientes, sino que además se dispone de una gran flexibilidad para la selección y las posibilidades de combinación de los protocolos de red utilizados.

Regla de filtro de paquetes

Con las reglas de filtro de paquetes se define si un paquete de datos puede pasar o no el filtro de paquetes. La decisión de si un paquete puede pasar o no se toma en base a campos de protocolo. Ejemplos de campos de protocolo son la dirección IP de origen y la dirección IP de destino. En el SCALANCE S se pueden indicar reglas de filtro para protocolos MAC o IP.

Regla de filtro de paquetes MAC

Por medio de reglas de filtro de paquetes MAC se pueden filtrar telegramas MAC.

Router NAT/NAPT

Con esta técnica se consigue que las direcciones de las estaciones de la subred interna no se conozcan en la red externa; en la red externa sólo se pueden ver a través de las direcciones IP externas definidas en la lista de conversión.

RSA

Rivest, Shamir & Adleman Algorithm

Se trata de un sistema criptográfico que se puede utilizar tanto para la encriptación como para la firma digital. Emplea una pareja de claves formada por una clave privada, utilizada para la desencriptación o la firma de datos, y una clave pública con la que se encripta o se comprueban firmas de datos. La clave privada se mantiene en secreto y su obtención a partir de la clave pública es imposible, o al menos extremadamente difícil.

Secure Hash Algorithm 1

Algoritmo para la verificación de datos

Security Configuration Tool

SCT

Herramienta de configuración para productos SCALANCE S.

Server

Un server (o servidor) es un equipo, o en general un objeto, capaz de prestar determinados servicios; a petición de un -> Client (cliente) se presta el servicio.

Servicios

Servicios ofrecidos por un protocolo de comunicación.

SHA1

Secure Hash Algorithm 1

Una función criptográfica de hash muy difundida. En el caso del SCALANCE S se puede seleccionar SHA1 para la prueba de integridad de los datos que se transmiten en un túnel.

SIMATIC NET

Siemens SIMATIC Network and Communication. Denominación de producto para redes y componentes de red de Siemens. (antes SINEC)

SNAP

Subnetwork Access Protocol

Mecanismo para multiplexar protocolos en redes que usen IEEE 802.2 LLC.

SOHO

Small Office, Home Office

SSN = DMZ

Secure Server Net = Demilitarized Zone

Stateful Packet Inspection

Stateful Inspection (también Stateful Packet Filter o Dynamic Packet Filter) es una tecnología de firewall y trabaja tanto a nivel de red como a nivel de aplicación. Los paquetes IP se reciben en el nivel de red, son inspeccionados en función del estado por un módulo de análisis y se comparan con una tabla de estados. Para el interlocutor de una comunicación, un firewall con Stateful Inspection representa una línea directa por la que sólo se permite el paso de una comunicación conforme a las reglas.

Syslog

Un servicio que recibe mensajes del sistema en un servidor (Syslog-Server) y los registra, por ejemplo, en archivos Log.

TACACS

Terminal Access Controller Access Control System; El Terminal Access Controller Access Control System (TACACS) es un protocolo AAA. Sirve para la comunicación Cliente-Servidor entre servidores AAA y un Network Access Server (NAS). Los servidores TACACS proporcionan una instancia de autenticación para usuarios remotos que deseen establecer una conexión IP con un NAS.

Tráfico IP

Designa la comunicación en redes informáticas que usa el protocolo IP como protocolo de red.

Túnel

Se entiende por túnel (o 'tunneling') el uso del protocolo de comunicación de un servicio de red como medio de transporte para datos no pertenecientes a dicho servicio.

Índice alfabético

A

Actualización del firmware, 38
Administración de usuarios, 113, 118
Advanced Mode, 108, 232
Ajuste de fábrica, 22
ajustes de red
    de un módulo, 133
Ajustes de Security, 203
Ajustes IKE, 186, 187
Ajustes IPSec, 186, 188
Alimentación de tensión, 17
Alimentación eléctrica, 20
Aplicaciones estándar, 17
Asignaciones a grupos, 113
Ausencia de retroacción, 13, 15
Authentication
    User, 118
Autocrossing, 20
Autonegotiation, 20

B

Barra de menús, 111
Bloque de bornes, 18
bloques de reglas IP, 142
bloques de reglas MAC, 142
bloques de reglas para firewall
    globales,, 114
Broadcast, 182

C

cable de Ethernet
    cruzado,, 20
cargar, 124
Caso de recambio, 36
CD, 19, 109
CD SCALANCE S, 109
Certificate, 182
Codificación, 109, 117
Codificación IPSec, 13, 15
Comandos de menú, 111
Condiciones del entorno/compatibilidad electromagnética, 25
Conectores RJ-45, 19
Conexiones, 25, 125
configuración
    cargar, 31
    primera, 31
Configuración de fábrica, 32
configurar offline, 31
Contacto de señalización, 18, 21
Conversión de direcciones, 165
C-PLUG, 16, 35
    no escrito, 36
    Reponer, 37
    retirar, 37

D

datos de proyecto
    coherentes,, 109
Datos eléctricos, 25
DCP (Primary Setup Tool), 159
Dead-Peer-Detection (DPD), 192
Default Router, 133
Derechos de Administrador, 38
DHCP
    Nombres simbólicos ("Symbolic Names"),
Dirección MAC, 31, 36, 133, 134
    en Routing Modus, 134
    impresa, 134
Distribución de carga, 21
Duración de certificados, 184

E

Equipo de recambio, 36
Espionaje de datos, 11, 14
Estado a la entrega, 32

F

Firewall, 13, 15, 135
    Nombres simbólicos ("Symbolic Names"),
    Preajuste, 138
    Reglas de Firewall, 130
    Reglas predefinidas, 137
Firewall para telegramas Ethernet-Non-IP

según IEEE 802.3,
Función MDI /MDIX Autocrossing, 20
Funciones de aprendizaje, 13, 194
Funciones de programación por aprendizaje, 15
Funciones de túnel, 179

G

gama de temperatura
ampliada,, 18
Grado de protección, 17
Grupo, 183
Grupo de servicios, 159
Grupos de servicios, 159

H

Hardware, 17
Homologaciones, 17
Homologaciones ver Normas, homologaciones, 26
Hora local del PC, 161
HTTPS (SSL), 139

I

ICMP Services, 153
IEEE 802.3, 130
IKE, 186, 187
Independencia de protocolo, 13
Indicador Fault (F), 24
Indicador Power (L1, L2), 24
Indicadores, 24
Indicador de error, 24
Indicadores de estado de puerto, 24
Interfaces TP, 19
IP-Firewall con Stateful Packet Inspection, 130

L

Logging
Clases de eventos, 230
Longitudes de cables, 25
Lugar de enchufe del C-PLUG, 35

M

MAC Rules, 155
Manipulación de datos, 11
Máscara de subred, 133
MD 740
Certificado de grupo, 126
Certificado de módulo, 126
Crear archivo de configuración, 126
Medio intercambiable
C-PLUG, 16
Método de autenticación, 181, 186
Misión de SOFTNET Security Client, 13
Modo de aprendizaje, 195
Modo Router, 15
Modo VLAN, 182
Módulo
crear, 132
Montaje, 27
Desmontaje, 28
Montaje en riel de perfil, 30
Montaje en riel perfil de sombrero, 28
Montaje mural, 30, 31
Tipos de montaje, 27
Montaje mural, 27, 30
Multicast, 182

N

NAT/NAPT, 165
National Electrical Code,table 11 (b), 20
Network Address Port Translation, 168
Network Adress Translation, 167
Nodos de red
no programables, 198
Nodos externos, 14, 16
Nodos internos, 14, 16
Nombre del grupo, 151, 157
Nombres simbólicos ("Symbolic Names"),
Normas, homologaciones, 26
ATEX 95, 27
EN 50021, 27
EN61000-4-5, 27
IEC950/EN60950/ VDE0805, 20

O

Offline, 108
Online, 108

P

Panorámica de funciones
Tipos de equipos, 18
Parámetros de dirección, 133
Parámetros de servicios MAC, 157
Posibilidades de conexión, 19

Preshared Keys, 182
Protección de acceso, 16
Protocolo ESP, 139
Proyecto, 113
  crear, 115
  valores de inicialización, 115
prueba de coherencia ("Check Consistency")
  a nivel de proyecto ~,
  local ~,
Prueba de coherencia ("Check Consistency"),
Puesta a tierra, 31
Puesta en servicio, 31
Pulsador Reset, 22

R

Recursos de software, 25
Referencias de pedido, 26
Reglas básicas de Firewall, 32
Reglas de filtrado de paquetes IP, 147
Reglas de Firewall globales, 130, 142
Reglas de Firewall locales, 130
Reglas para filtrado de paquetes MAC, 154
Reposición a la configuración de fábrica, 23
Riel de perfil, 27, 30
Riel de perfil S7, 31
Riel perfil de sombrero, 17, 27, 28
Router, 133
  externo, 134
  Router NAT/NAPT, 131
  Standard, 134
Router NAT/NAPT
  Nombres simbólicos ("Symbolic Names"),
Router NAT/NAPT, 165
Routing Modus, 134

S

Security Configuration Tool, 16, 107
  Barra de menús, 111
  Modos de funcionamiento, 108
  Vistas de operación, 108
Security Module SCALANCE S, 11
Sello horario
  de entradas en Log, 161
Servicios IP, 150
Servidor DHCP, 131
  configuración, 174
Servidor NTP, 161
SiClock, 159
SOFTNET Security Client, 13
  Base de datos, 206
  Cargar por lectura datos de configuración, 209
  Comportamiento de arranque, 204
  desinstalar, 205
  Enable active learning, 215
  Entorno de uso, 203
SSL Certificate, 163
Standard Mode, 108, 231
Stateful Packet Inspection, 130
Syslog
  Nombres simbólicos ("Symbolic Names"),

T

Tabla de símbolos, 121
Tapa roscada M32, 35
Telegramas Layer 2, 13, 15
Telegramas Non-IP, 181
Tensión alterna, 21
Túnel, 179
Túnel IPsec, 13, 179
Túnel VPN, 13, 15

U

User
  configurar, 118
usuarios
  autorizados,, 109

V

VLAN-Tagging, 182
Volumen de suministro, 18
VPN, 13, 15
  Porpiedades específicas del módulo, 191
  SOFTNET Security Client, 201

W

Windows 2000, 109
Windows XP / SP1 o SP2, 109